EXHIBIT 8

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

FRCP 26(a)(2)(B) Expert Report of Kevin T. Faulkner

HUNTERS CAPITAL, LLC, et al
vs.
CITY OF SEATTLE,

Case No. 2:20-cv-00983 TSZ

Introduction

Engagement Background

Palo Alto Networks, Inc. ("Palo Alto Networks") was initially retained by outside counsel on behalf of its client, the City of Seattle (the "City") on November 5, 2020, to provide digital forensic investigative services in connection with pending and anticipated litigation, including *Hunters Capital, LLC, et al v. City of Seattle*, No. 2:20-cv-00983 (W.D. Wash. 2020). The Unit 42 Security Consulting group ("Unit 42") at Palo Alto Networks, formerly known as Crypsis, performed the services in this engagement.

Unit 42 initiated its investigation on November 5, 2020, beginning with a remote investigation and then an on-site collection of data on November 19, 2020.

I, Kevin T. Faulkner, have been asked to prepare a report describing this investigation, and hereby submit the following report pursuant to FRCP 26(a)(2)(B). When I refer to actions taken by myself or Unit 42 in this report, those actions were taken by me and/or Unit 42 personnel who were working at my direction. All dates and times discussed in this report are presented in Coordinated Universal Time ("UTC"), unless otherwise noted.

Experience and Qualifications

I am a vice president in the Unit 42 Security Consulting group at Palo Alto Networks. Unit 42 Security Consulting specializes in digital forensic investigations, data breach and computer crime response, and digital risk management services. In my capacity as a vice president, I lead and perform digital forensic and incident response investigations and other risk management engagements on behalf of Palo Alto Networks' clients. I regularly supervise and perform digital forensic acquisitions and examinations of laptop and desktop computers, email and file servers, handheld/mobile devices, backup tapes, and network logs in civil and criminal cases, internal investigations, and cybercrime engagements.

Palo Alto Networks acquired The Crypsis Group in September of 2020 and merged the team from Crypsis with the Unit 42 team under the name Unit 42 Security Consulting.

Prior to my employment by Crypsis and Palo Alto Networks, I served as a managing director and head of the national digital forensics and incident response practice at Stroz Friedberg, where I co-managed the firm's technical operations in the areas of digital forensics and incident response.

I have over 18 years of experience in digital forensics and incident response, and over 23 years of experience in technology consulting. I have attained a number of certifications in digital forensics, computer security, and information technology including: Certified Computer Examiner ("CCE"), EnCase Certified Examiner ("EnCE"), GIAC Certified Forensic Examiner ("GCFE"), Payment Card Industry ("PCI") Qualified Security Assessor ("QSA"), CompTIA Linux+, and Microsoft Certified Professional ("MCP").

I have testified and submitted affidavits, declarations, witness statements, and/or expert reports in my capacity as a digital forensic expert approximately 70 times. In the last 10 years I have offered testimony in the following courts:

- Connecticut Superior Court, Hartford, Complex Litigation
- District Court of Rotterdam
- Kosciusko County Superior Court 4, State of Indiana
- New Jersey Superior Court, Somerset County - Law Division
- Superior Court of The State of California, County of Los Angeles, Central District

- Supreme Court of The State of New York, County of New York
- The United States Bankruptcy Court, District of Delaware
- The United States District Court for the District of Massachusetts
- The United States District Court for the Eastern District of New York
- The United States District Court for the Eastern District of Pennsylvania
- The United States District Court for the Northern District of California
- The United States District Court for the Northern District of New York
- The United States District Court for the Southern District of New York
- The United States International Trade Commission, Washington D.C.

Attached to this report as Exhibit 1 is a true and correct copy of my curriculum vitae, which sets forth a detailed list of my background, qualifications, and testimony experience.

Compensation

Palo Alto Networks is being compensated for my work on this case at the rate of $550 per hour for my professional services in this matter. Certain members of my team at Unit 42 who are working at my direction on this matter are billing between $300 and $550 per hour. Palo Alto Networks also charges $700 per hour for expert testimony. Neither Palo Alto Networks' nor my compensation depends in any way on the outcome of this matter or the substance of my opinions or testimony.

Materials Considered

The materials that I considered in forming the opinions set forth in this report include my over 18 years of experience as a digital forensics expert, all references cited in this report, and the list of materials attached as Exhibit 2 to this report.

Reservation of Rights

I reserve the right to supplement or amend my opinions or this report at any time prior to the expert disclosure deadlines in the case, in response to opinions expressed by other experts, or in light of any additional evidence, testimony, discovery, court rulings, or other information that may be provided to me after the date of this report. In addition, I reserve the right to consider and testify about issues that may be raised by fact witnesses and experts at trial.

In connection with any testimony that I am asked to provide in this matter, I may use as exhibits various documents produced in this matter that refer or relate to the topics discussed in this report. In addition, I reserve the right to use animations, demonstratives, enlargements of exhibits, and other information to convey my opinions and the bases for them, as appropriate.

Executive Summary

Purpose of Our Engagement

The City identified that a number of mobile phone text messages could not be found on mobile devices issued by the City to former Seattle Mayor Jenny A. Durkan ("Mayor Durkan") and former Seattle Police Chief Carmen Best ("Chief Best").[1] The time frame in which text messages initially could not be located for Mayor Durkan was between August 29, 2019, and June 25, 2020 (the "Initial Missing Durkan Text Messages"). During this time frame, extending to when Unit 42 began assisting with this investigation, Mayor Durkan used three different mobile phones at different points in time, which are described in this report in the section entitled, "Devices Used by Mayor Durkan." The time frame in which text messages could not be located for Chief Best was prior to September 2, 2020 (the "Missing Best Text Messages"). During the time period from October 1, 2019, to September 2, 2020, Chief Best used one City-issued mobile phone.

The goals of this investigation were to:

1. Attempt to recover or otherwise locate the missing text messages of Mayor Durkan and Chief Best.

2. Determine what happened to cause the text messages of Mayor Durkan and Chief Best to be missing.

One aspect that was not a focus of this investigation was to assess who made any changes to settings on the mobile phones of Mayor Durkan and Chief Best that may have been made. Data extracted from mobile phones can typically reveal to forensic investigators how the device was configured. In some instances, there is information that may show when certain changes were made. But, typically, digital forensic evidence would not show what specific person made any changes. Therefore, investigating who made changes was outside the scope of Unit 42's investigation.

Summary of Findings

Mayor Durkan

During the course of Unit 42's investigation, the iPhone 8 Plus (Verizon) (as later defined), which initially could not be located, was found by City employees on June 28, 2021, and provided to Unit 42 for analysis. Locating the iPhone 8 Plus (Verizon) filled in some of the Initial Missing Durkan Text Messages being sought, specifically from August 29, 2019, through October 30, 2019. Accordingly, following Unit 42's investigation, the time frame in which text messages have not been located or recovered is October 30, 2019, through June 25, 2020 (the "Missing Durkan Text Messages").

Unit 42 determined that the Missing Durkan Text Messages (those sent or received between October 30, 2019, and June 25, 2020) were not recoverable from Mayor Durkan's mobile devices and could not be found in the data sources related to Mayor Durkan. The sources of data related to Mayor Durkan that were examined in this investigation are detailed in the section of this report entitled "Mayor Durkan Data Sources" and include backups of mobile devices taken at different points in time, data from Apple iCloud, and multiple forensic extractions of mobile devices from different points in time that were created using multiple forensic tools.

Artifacts from Mayor Durkan's data sources indicate that, at an unknown point in time on or after July 4, 2020 PDT, and before the next configuration change occurred between July 22, 2020 PDT and July 26, 2020 PDT,[2] the "Message History" setting on either Mayor Durkan's iPhone 8 Plus (FirstNet) or her iPhone

[1] When the City initially retained Unit 42 in November 2020, the scope of work was only to investigate the Initial Missing Durkan Text Messages. Later, when the City discovered that Chief Best was missing text messages as well, our scope of work expanded to include Chief Best.

[2] The artifacts Unit 42 reviewed are consistent with the "Message History" setting having changed from "30 Days" to "Forever" between July 23, 2020, at 06:11:47 UTC and July 26, 2020, at 10:00:00 UTC, (July 22, 2020, at 23:11:47

11 (FirstNet) (as later defined) likely had been set to "Keep Messages" for "30 Days." Then, between July 22, 2020 PDT and July 26, 2020 PDT, the "Message History" setting on the iPhone 11 (FirstNet) likely was reconfigured to "Keep Messages" "Forever." When the setting is configured to "Keep Messages" for "30 Days," any text messages older than 30 days stored locally on an iPhone are automatically deleted by the iPhone on a nightly, rolling basis. We investigated whether there were any events that could have changed the text message retention settings without manual intervention, and to date have not identified any that apply. This investigation did not assess who may have changed settings on Mayor Durkan's phones, as digital forensic evidence regarding who made changes does not typically exist on mobile devices.

Mayor Durkan's iPhone 8 Plus (Verizon), in use from April 2018 to October 2019, contained text messaging data from November 18, 2017, to October 30, 2019. A backup of Mayor Durkan's iPhone 11 (FirstNet), in use since July 2020, was identified on the computer of Michelle Chen ("Ms. Chen"), a City employee working in the Mayor's office. This backup was dated August 21, 2020, and contained text messaging data from June 25, 2020, to August 21, 2020. The Missing Durkan Text Messages fall in the date range between these two data sets (October 30, 2019, to June 25, 2020) for which no additional data sources containing text messages related to Mayor Durkan's iPhones have been identified. Text messaging data from June 25, 2020, and forward has been preserved through multiple collections of data.

Chief Best

Analysis of the Best iPhone XS Max (as later defined) led to the identification of two backups of older iPhones used by Chief Best; however, none of the data sources found filled in any of the Missing Best Text Messages from the summer of 2020, which Unit 42 understands to be the relevant time period for this litigation. The two backups did provide some text messages from 2017 and 2019, but no additional messages from 2020.

The sources of data related to Chief Best that were examined in this investigation are detailed in the section of this report entitled "Chief Best Data Sources." These data sources include backups of mobile devices taken at different points in time and forensic extractions from the iPhone Chief Best most recently used.

Ultimately, our analysis showed that Chief Best's iPhone XS Max contained information in the text message database that was consistent with her deposition testimony that she deleted text messages periodically.

Devices Used by Mayor Durkan

Mobile Devices

Unit 42 understands that Mayor Durkan used three different mobile devices from April 2018 to November 2020. This understanding is based on analysis of the devices, analysis of backups from the devices, and statements made by City employees. Unit 42 currently has custody of these three mobile devices, which are stored in our evidence storage facility. Details about the three mobile devices are provided below:

1. An iPhone 8 Plus, model: A1864, serial number: F17WDNB4JCLM, on the Verizon cellular network, used from April 10, 2018, through October 30, 2019, (the "**iPhone 8 Plus (Verizon)**")

2. An iPhone 8 Plus, model: A1897, serial number: FD1XR5Y8JCM2, on the FirstNet cellular network built with AT&T, used from October 30, 2019, through July 9, 2020, (the "**iPhone 8 Plus (FirstNet)**")

3. An iPhone 11, model: A2111, serial number: F4GCQQ6PN72Q, on the FirstNet cellular network built with AT&T, used from July 9, 2020, through November 19, 2020, (the "**iPhone 11 (FirstNet)**")

PDT and July 26, 2020, at 03:00:00 PDT). The "Message History" setting was set to "30 Days" between the point in time when the "Disable & Delete" function was used on July 4, 2020 PDT, and the point in time when it was set back to "Forever" between July 22, 2020 PDT and July 26, 2020 PDT.

Unit 42 further understands that Mayor Durkan was provided a new mobile device on November 19, 2020, when Unit 42 took custody of the iPhone 11 (FirstNet). This new mobile device has not been examined by Unit 42.

The following image depicts a timeline of the iPhone mobile devices used by Mayor Durkan from early 2018 to late 2020 with pins showing the dates when devices went into or were taken out of use.

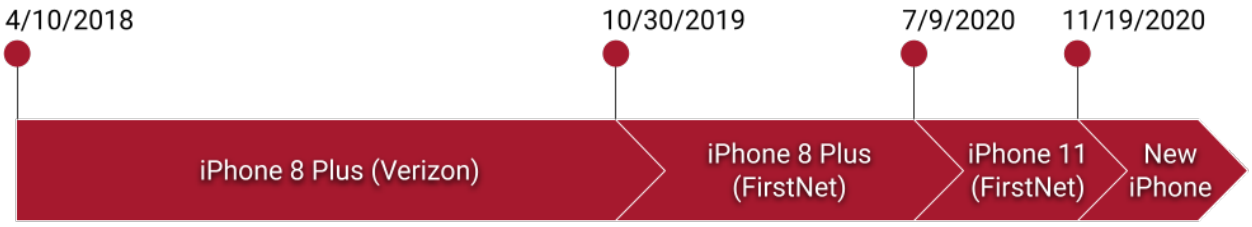


Figure 1 - Timeline of Durkan Mobile Device Usage

Computer Devices

In addition to the mobile devices, Mayor Durkan used two computer laptop/tablet devices provided by the City. Details about these two devices are provided below:

1. A Microsoft Surface Pro 4, serial number: 048165462053, which was described as the tablet Mayor Durkan uses from home for City-related work

2. A Microsoft Surface Pro 7, serial number: 030612294353, which was described as the tablet Mayor Durkan uses from the office for City-related work

On-Site Inspection and Collection

Unit 42 vice president, Kevin T. Faulkner, traveled to Seattle and on November 19, 2020, met with team members from the City, collected data and devices, and inspected other devices not necessary for collection.

Mr. Faulkner took custody of two of Mayor Durkan's iPhones on November 19, 2020. At the time of Mr. Faulkner's visit, the iPhone 11 (FirstNet) was Mayor Durkan's current phone. The City's IT team provided Mayor Durkan with a new iPhone and transferred data from the iPhone 11 (FirstNet) to the new iPhone. Once the City's IT team completed transferring data onto the new iPhone, Mr. Faulkner took custody of the iPhone 11 (FirstNet). While on-site, Mr. Faulkner also took custody of the iPhone 8 Plus (FirstNet), which Mayor Durkan used prior to the iPhone 11 (FirstNet). The iPhone 8 Plus (Verizon) was not collected while Mr. Faulkner was on-site, as the City team was still working to identify its location.

On November 19, 2020, Mr. Faulkner also inspected the two City-owned Microsoft Surface Pro computers assigned to Mayor Durkan, looking for any evidence of iPhone backups on those two computers. Neither computer was found to have the Apple iTunes software installed and no iPhone backups were found on either of these two computer systems.

On June 28, 2021, a City employee located Mayor Durkan's iPhone 8 Plus (Verizon). It was shipped to Unit 42's forensics lab and was received by the Unit 42 team on July 2, 2021.

Mayor Durkan Data Sources

For the three mobile devices used by Mayor Durkan, there were multiple sources of data that Unit 42 collected and analyzed in this investigation, which were provided to plaintiffs and/or their expert. This section describes all of the sources of data related to Mayor Durkan that were considered in this investigation, which are collectively referred to in this report as the "Durkan Data Sources." In addition to data extracted directly from the mobile devices, Unit 42 also collected and analyzed backup preservations

of the devices created with iTunes. Ms. Chen had indicated during prior meetings that her computer likely contained backups of potentially relevant iPhone devices from Mayor Durkan. In order to capture the potentially relevant backups along with information sufficient to analyze how and when backups were taken and what may have been done with the data, Unit 42 forensically imaged Ms. Chen's computer using a Logicube Falcon-Neo forensic imaging device on November 19, 2020.

These Durkan Data Sources are described below, grouped by the mobile device to which the data source relates. It is important to note that the date that data was collected does not necessarily represent the date that is reflected in that data source. For example, if a backup was collected three months after it was taken, the data source represents the configuration and data on that mobile device as of the date the backup was taken, not when the backup was collected. Similarly, if a mobile device was taken out of use and then collected over a year later, the data source may represent the configuration and data on that mobile device when it was taken out of use rather than when it was actually collected.

iPhone 8 Plus (Verizon)

- An iTunes backup dated August 29, 2019, was identified on Ms. Chen's computer. Unit 42 preserved a forensic image of Ms. Chen's computer while on-site on November 19, 2020. The backup represents the configuration and data on the phone as of the date the backup was taken, August 29, 2019.

- On July 2, 2021, after receiving the iPhone 8 Plus (Verizon), Unit 42 created an advanced logical data extraction[3] using forensic software from Cellebrite. This data extraction represents the configuration and data on the iPhone 8 Plus (Verizon) as of October 30, 2019, because that is the date when the phone was taken out of use.

- On July 7, 2021, Unit 42 created a full file system[4] data extraction using forensic software from Cellebrite. This data extraction also represents the configuration and data on the iPhone 8 Plus (Verizon) as of October 30, 2019, because that is the date when the phone was taken out of use. A full file system data extraction contains additional information and data from a mobile device not captured in an advanced logical data extraction.

The following image depicts a timeline when the iPhone 8 Plus (Verizon) was in use from April 10, 2018, through October 30, 2019. The red pins represent when data preservations exist, reflecting the phone's configuration and data as of August 29, 2019, and October 30, 2019.

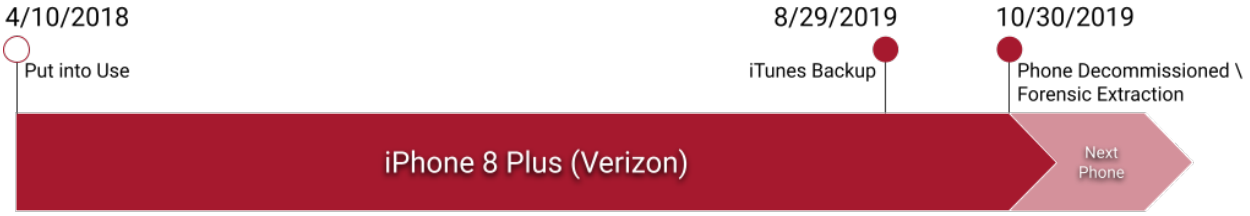


Figure 2 - Timeline of iPhone 8 Plus (Verizon) Durkan Data Sources

[3] An advanced logical extraction was performed using Cellebrite. This method collects a subset of data, such as text/chat messages, call history, photos, contacts, and configuration information.

[4] A full file system extraction was performed using Cellebrite with the checkm8 method, allowing a deeper level of access to the system partition, application data, and other files that would not typically be accessible for preservation with an advanced logical extraction.

iPhone 8 Plus (FirstNet)

- On November 17, 2020, Unit 42 received a mobile preservation that was performed by an "Information Security Engineer" with the City on September 18, 2020. The preservation was performed using forensic software from Magnet Forensics Inc., named "Magnet ACQUIRE." The City's "Information Security Engineer" reported that they had received the iPhone 8 Plus (FirstNet) in a factory-reset state and had to complete the setup of the device, which they did, in order to extract data. This preservation represents the configuration and data of the iPhone 8 Plus (FirstNet) on September 18, 2020, after the device had been factory reset and subsequently set up. Because this device was in a factory-reset state, any settings or data related to prior use of this phone were no longer present on the device and were therefore not captured in this data extraction.

- While on-site in Seattle on November 19, 2020, Unit 42 created an advanced logical extraction using forensic software from Cellebrite. This preservation effectively represents the data and configuration of the iPhone 8 Plus (FirstNet) on September 18, 2020, because that is when the device was set up after an earlier reset. Because this device was in a factory-reset state, any settings or data related to prior use of this phone were no longer present on the device and were therefore not captured in this data extraction.

- On July 7, 2021, Unit 42 created a full file system data extraction of the iPhone 8 Plus (FirstNet) using forensic software from Cellebrite. This preservation effectively represents the data and configuration of the iPhone 8 Plus (FirstNet) on September 18, 2020, because that is when the device was set up after an earlier reset. Because this device was in a factory-reset state, any settings or data related to the prior use of this phone were no longer present on the device and were therefore not captured in this data extraction. A full file system data extraction contains additional information and data from a mobile device not captured in an advanced logical data extraction.

- None of the forensic extractions of data from the iPhone 8 Plus (FirstNet) (neither the collection on September 18, 2020, the advanced logical extraction on November 19, 2020, nor the full file system data extraction on July 7, 2021) contained any information from the device when it was in use by Mayor Durkan because the device had been factory reset. Furthermore, no backups for the iPhone 8 Plus (FirstNet) were located within any other Durkan Data Sources. Analysis by Unit 42 did confirm that, on July 9, 2020, data from the iPhone 8 Plus (FirstNet) was transferred to the iPhone 11 (FirstNet). Therefore, any information found on the iPhone 11 (FirstNet) that predates July 9, 2020, is actually data from the iPhone 8 Plus (FirstNet) that was transferred over when the iPhone 8 Plus (FirstNet) was replaced. For this reason, all of the Durkan Data Sources listed below for the iPhone 11 (FirstNet) may also be considered as data sources for the iPhone 8 Plus (FirstNet) to the extent that information can be identified as something that had been transferred over from before July 9, 2020.

The following image depicts a timeline when the iPhone 8 Plus (FirstNet) was in use from October 30, 2019, through July 9, 2020, and further to September 18, 2020. The red pin represents when data preservations exist reflecting the phone's configuration and data as of September 18, 2020.

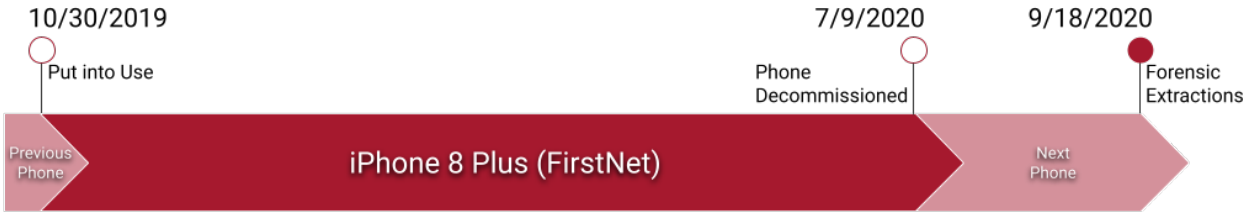


Figure 3 - Timeline of iPhone 8 Plus (FirstNet) Durkan Data Sources

iPhone 11 (FirstNet)

- An iTunes backup of the iPhone 11 (FirstNet) dated August 21, 2020, was identified on Ms. Chen's computer. Unit 42 preserved Ms. Chen's computer on November 19, 2020. The backup represents the configuration and data on the iPhone 11 (FirstNet) as of August 21, 2020.

- On November 17, 2020, Unit 42 received a mobile preservation that was performed by an "Information Security Engineer" with the City on October 15, 2020. The preservation was performed using Magnet ACQUIRE. This preservation represents the configuration and data on the iPhone 11 (FirstNet) as of October 15, 2020.

- While on-site in Seattle on November 19, 2020, Unit 42 created an advanced logical extraction using forensic software from Cellebrite. This preservation represents the configuration and data on the phone as of November 19, 2020, when the phone was taken out of use after transferring its data to a new iPhone.

- On July 8, 2021, Unit 42 created a full file system extraction using the unc0ver jailbreak and forensic software from Belkasoft LLC.[5] This collection represents the configuration and data on the phone as of November 19, 2020, as the phone was taken out of use on that day. A full file system data extraction contains additional information and data from a mobile device, not captured in an advanced logical data extraction.

The following image depicts a timeline when the iPhone 11 (FirstNet) was in use from July 9, 2020, through November 19, 2020. The red pins represent when data preservations exist reflecting the phone's configuration and data as of August 21, 2020, October 15, 2020, and November 19, 2020.

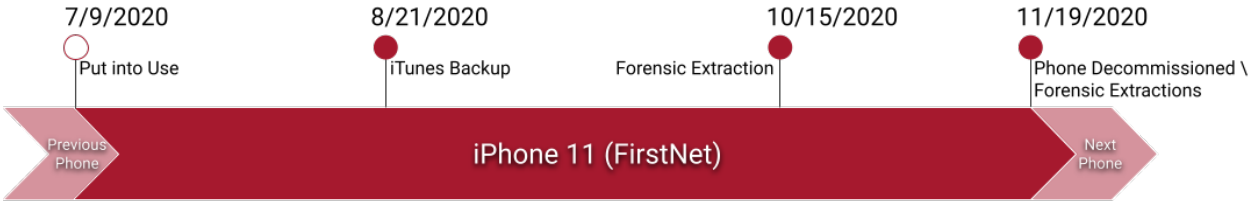


Figure 4 - Timeline of iPhone 11 (FirstNet) Durkan Data Sources

iCloud Account

- On November 16, 2020, Unit 42 collected data from Mayor Durkan's iCloud account that was used on all three of Mayor Durkan's iPhones used from 2018 to the time Unit 42 became involved in this investigation in November 2020. This iCloud account was examined, and data was collected on November 16, 2020, using Magnet Forensics Inc. AXIOM Cloud and Elcomsoft Ltd. Phone Breaker. These collections did not include text messages in iCloud, as the process to access text messages in iCloud using forensic software was producing an error due to the additional security around text messages in iCloud.

- On September 9, 2021, Unit 42 collected additional data from Mayor Durkan's iCloud account that was used on all three of Mayor Durkan's iPhones used from 2018 to the time Unit 42 became involved in this investigation in November 2020, as well as the new phone in use as of September 9, 2021. This iCloud account was examined, and data was collected on September 9, 2021, using Elcomsoft Phone Breaker. This collection included only account data and text messages in iCloud

[5] Performing the jailbreak process with unc0ver and acquiring the iPhone 11 (FirstNet) with Belkasoft was a different process for obtaining a full file system than was used on the two iPhone 8 Plus devices. This different process was necessary because the process used on the two iPhone 8 Plus devices was not compatible with iPhone 11 hardware.

to supplement the earlier collection on November 16, 2020.[6] The text message data collected from iCloud covered the date range of June 25, 2020, through September 9, 2021.

Computer Devices

- No data was collected from the two Microsoft Surface Pro computers issued by the City to Mayor Durkan. These devices were inspected on November 19, 2020, on-site in Seattle, and, because no mobile phone backups were found, no data was collected from these devices.

Pinnacle Data Extraction

- Pinnacle is a centralized database that receives billing and usage information from cellular provider companies used by the City. Unit 42 received an extraction of information from Pinnacle that contains, among other things, dates, times, and recipient information for traditional cellular network "SMS" text messages, but not for Apple proprietary "iMessage" text messages. The extraction contained records from the beginning of January 2020 through the end of August 2020 for Mayor Durkan's mobile phone number.

Devices Used by Chief Best

Mobile Devices

Unit 42 found that Chief Best used at least three different mobile devices from July 2016 to September 2020. This finding is based on the analysis of Chief Best's most recent iPhone and the analysis of backups from two older devices. Unit 42 currently has custody of Chief Best's most recent device that was used during the summer of 2020, which is stored in our evidence storage facility. Details about the three mobile devices are provided below:

1. An iPhone 6s Plus, model: A1687, serial number: F2LRMBLFGRWV, on the Verizon cellular network, used from July 18, 2016, through at least November 15, 2017, the date the backup of this device was taken, (the "**Best iPhone 6s Plus**").

2. An iPhone 8 Plus, model: A1864, serial number: FD6W12T6JCLY, on the Verizon cellular network, used from November 5, 2018, until October 1, 2019, (the "**Best iPhone 8 Plus**").

3. An iPhone XS Max, model: A1921, serial number: F2LZ5ANGKPHC, on the Verizon cellular network, used from October 1, 2019, through September 2, 2020, (the "**Best iPhone XS Max**").

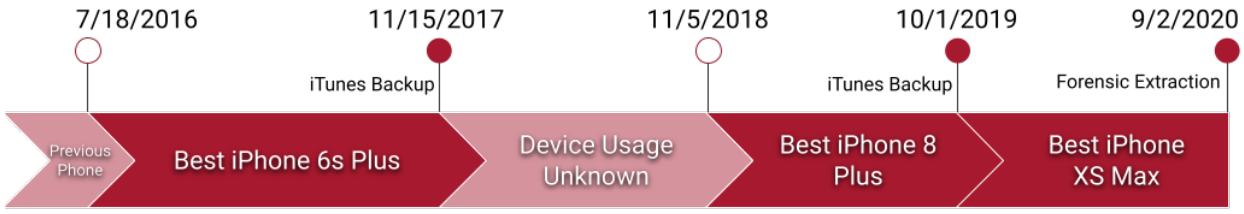


Figure 5 - Timeline of Best Mobile Device Usage

Chief Best Data Sources

For the mobile devices used by Chief Best, there were multiple sources of data that Unit 42 collected and analyzed in this investigation. This section describes the sources of data related to Chief Best considered in this investigation, which are collectively referred to in this report as "Best Data Sources." Unit 42

[6] Text message data in iCloud was obtained by authenticating with the additional security required to access text message data.

understands that Chief Best's last date of employment with the City was September 2, 2020, and that she turned in her City-issued iPhone on that day.

On February 24, 2021, ArcherHall, LLC. ("ArcherHall"), one of the City's vendors, collected an advanced logical data extraction using forensic software from Cellebrite from the mobile device last used by Chief Best. On October 22, 2021, Epiq Systems, Inc. ("Epiq"), another of the City's vendors, preserved a City-owned computer used by Chief Best's assistant, Tricia Colin ("Ms. Colin"). Unit 42 analyzed the forensic image of Ms. Colin's computer and identified two iTunes backups related to Chief Best.

These Best Data Sources are detailed below. It is important to note that the date that data was collected does not necessarily represent the date that is reflected in that data source. For example, if a backup was collected three months after it was taken, the data source represents the configuration and data on that mobile device as of the date the backup was taken, not when the backup was collected. Similarly, if a mobile device was taken out of use and then collected over a year later, the data source may represent the configuration and data on that mobile device when it was taken out of use, rather than when it was actually collected.

Best iPhone 6s Plus

- An iTunes backup of the Best iPhone 6s Plus dated November 15, 2017, was identified on a computer used by Ms. Colin. Epiq preserved Ms. Colin's computer on October 22, 2021. The backup represents the configuration and data on the Best iPhone 6s Plus as of November 15, 2017.

Best iPhone 8 Plus

- An iTunes backup of the Best iPhone 8 Plus dated October 1, 2019, was identified on a computer used by Ms. Colin. Epiq preserved Ms. Colin's computer on October 22, 2021. The backup represents the configuration and data on the Best iPhone 8 Plus as of October 1, 2019.

Best iPhone XS Max

- Unit 42 received an advanced logical data extraction performed by ArcherHall with forensic software from Cellebrite on February 24, 2021. This data extraction represents the configuration and data on the Best iPhone XS Max as of September 2, 2020, Chief Best's last date of employment, as that is when the iPhone went out of use.

- On November 8, 2021, Unit 42 created an additional advanced logical data extraction using forensic software from Cellebrite.

Computer Devices

- Analysis of the Best iPhone XS Max identified a connection to a computer named OC510093 with the username "colint." This computer was found to have been used by Ms. Colin, assistant to Chief Best, and was imaged by Epiq. The acquisition logs show that the hard drive from Ms. Colin's computer was a Seagate model ST500DM002, 500GB drive with the serial number ZA418CY4. Analysis of this computer found two iPhone backups related to two mobile devices used by Chief Best, specifically the Best iPhone 6s Plus and Best iPhone 8 Plus. Analysis also showed that the Best iPhone XS Max was connected to Ms. Colin's computer on October 1, 2019, the same day the Best iPhone 8 Plus was backed up, and that the Best iPhone XS Max was initially set up through a restore of data from the Best iPhone 8 Plus. There were no backups of the Best iPhone XS Max on this computer.

Background and Foundational Information

Information from People Knowledgeable

Unit 42 understands from discussions with Mayor Durkan's team that she used the iPhone 8 Plus (Verizon) until October 30, 2019, when it was replaced by the iPhone 8 Plus (FirstNet) in an attempt to get better

cellular reception at her home by switching carriers. She then used the iPhone 8 Plus (FirstNet) until July of 2020 when she reported that her phone was submerged in salt water for some period of time on July 4, 2020, causing problems with the phone, after previously having cracked the screen.[7] On July 9, 2020, the iPhone 8 Plus (FirstNet) was replaced with the iPhone 11 (FirstNet), which Mayor Durkan used until Unit 42 took custody of the device on November 19, 2020. This timeline is consistent with the Durkan Data Sources.

We also understand that Ms. Chen had a process whereby she backed up Mayor Durkan's iPhones at different points in time. Ms. Chen confirmed that she had performed her backup process on multiple phones in use by Mayor Durkan, over a period of time, but she did not have a regular cadence for making those backups. Ms. Chen's account of events is consistent with the timestamps observed within the Durkan Data Sources.

Unit 42 requested that the City's IT resources provide any backups or other data captures, to the extent any such backups exist, from Mayor Durkan's phones and learned that other than what Unit 42 collected as described herein, no additional backups had been made. Unit 42 understands that the City IT team's customary practice when migrating a user in the Mayor's office from one phone to another using the "Quick Start" feature was to create an iCloud backup of the source phone prior to performing the migration. We also understand that after the data was transferred from the iPhone 8 Plus (FirstNet) to the iPhone 11 (FirstNet), the City IT team reset the iPhone 8 Plus (FirstNet) to factory defaults, as was its customary practice, which would have removed all prior configuration settings and data from the device, about one month after the Mayor switched to the iPhone 11 (FirstNet).

Unit 42 also learned that a system called Pinnacle may contain limited metadata related to text messaging. Pinnacle is a centralized database that receives billing and usage information from cellular provider companies used by the City. For some cellular providers, this usage information includes the dates and times of text messages routed over the cellular provider's network, along with the phone numbers involved in the text message exchanges.

Mobile Device Forensic Artifacts

Mobile devices, such as the iPhones used by Mayor Durkan and Chief Best, do not generally keep a log detailing the history of everything that happened on that device. Forensic investigators must analyze numerous configuration files, logs, databases, and other information to piece together or infer what happened on a mobile device. A forensic artifact is a piece of data that can be used to understand the configuration of a setting or the occurrence of something that happened. Each of the forensic artifacts relied upon to attempt to reconstruct and understand what happened on the mobile devices issued to Mayor Durkan and Chief Best often consist of just one entry, or a few entries, in a file with dozens or hundreds of other entries.

This section of the report describes many of the forensic artifacts used in the analysis of Mayor Durkan's and Chief Best's iPhones, and describes what those artifacts are called, where they are stored, how they work, and how the meaning of their values can be interpreted. If other artifacts come to light or additional analysis of these or other artifacts identifies any new findings or changes any conclusions, Unit 42 reserves the right to supplement or amend this report.

iPhone Setup Information

On an iPhone, a configuration file named "com.apple.MobileBackup.plist" contains information related to the setup or "restore" of the device. An iPhone, when being set up, can be configured as a new, blank device, or it can be restored with data from another iPhone in multiple ways, including from an iTunes backup on a computer, an iCloud backup[8] stored on Apple's servers, or by "Quick Start," which transfers

[7] Mayor Durkan 12/8/2021 Dep. Tr. at 255:7-259:24.
[8] For more information about the iCloud backup process, see https://support.apple.com/en-us/HT207428.

data from one iPhone directly to another.[9] The file "com.apple.MobileBackup.plist" is typically located in the "/private/var/root/Library/Preferences" folder. Depending on the restore options selected during setup, different key and value pair combinations will exist in the "com.apple.MobileBackup.plist" file.

The "RestoreDate" key contains a value that represents the last date and time that a restore occurred. The "WasCloudRestore" key has a value of "True" if the device was restored from an iCloud backup or "False" if it was not. If data was transferred using the "Quick Start" feature, a key named "SourceDeviceUDID" will exist, and its value records a unique device identifier for the source iPhone from which data was transferred to the destination iPhone. Another value, "FileTransferStartDate," records the start date and time of the data transfer.

The figure below shows a limited preview of the contents of the "com.apple.MobileBackup.plist" configuration file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), which was identified on Ms. Chen's computer.

Figure 6 - A screenshot of a limited preview of the "com.apple.MobileBackup.plist" file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Another configuration file, "com.apple.purplebuddy.plist," has a key/value pair named "SetupLastExit," which records the date that the setup application completed. This configuration file is typically located in the "/private/var/mobile/Library/Preferences" folder.

The following figure shows a limited preview of the contents of the "com.apple.purplebuddy.plist" configuration file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), which was identified on Ms. Chen's computer.

[9] This Apple article details options for transferring data from one iPhone (or Android device) to another iPhone: https://support.apple.com/en-us/HT202033.

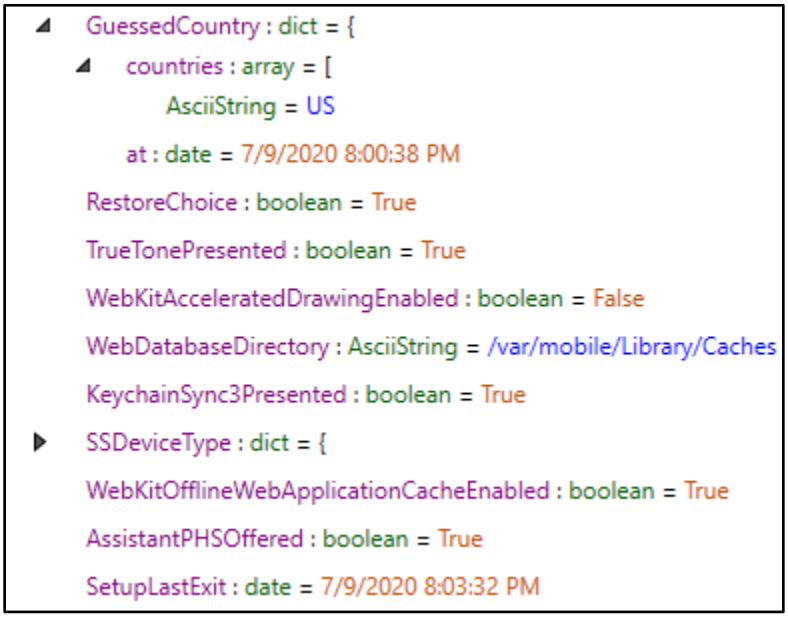


Figure 7 - A screenshot of a limited preview of the "com.apple.purplebuddy.plist" file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Additionally, a configuration file named "com.apple.mobileSMS.plist" records information related to the "Messages in iCloud" feature, but some of the key/value pairs in this file can also relate to how the device was set up. This configuration file is typically located in the "/private/var/mobile/Library/Preferences" folder.

The "IMDSavedDeviceStateDidRestoreFromCloudBackupKey" key has a value of "True" or "False" to indicate whether or not a key needed for synchronizing message data was retrieved from an iCloud backup. If the value is "True," another key, named "IMDSavedDeviceStateDateKey," records when the event occurred. Additionally, the key "IMDSavedDeviceStateDidMigrateFromDifferentDeviceKey" will have a value of "True" or "False" to indicate if the iCloud backup that was restored was from the same (True) or a different (False) device. These artifacts can be used to determine if/when a device was restored from an iCloud backup, when the restore occurred, and whether or not it was a restore of a backup from a different device.

The figure below captures the contents of the "com.apple.mobileSMS.plist" configuration file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) which was identified on Ms. Chen's computer.

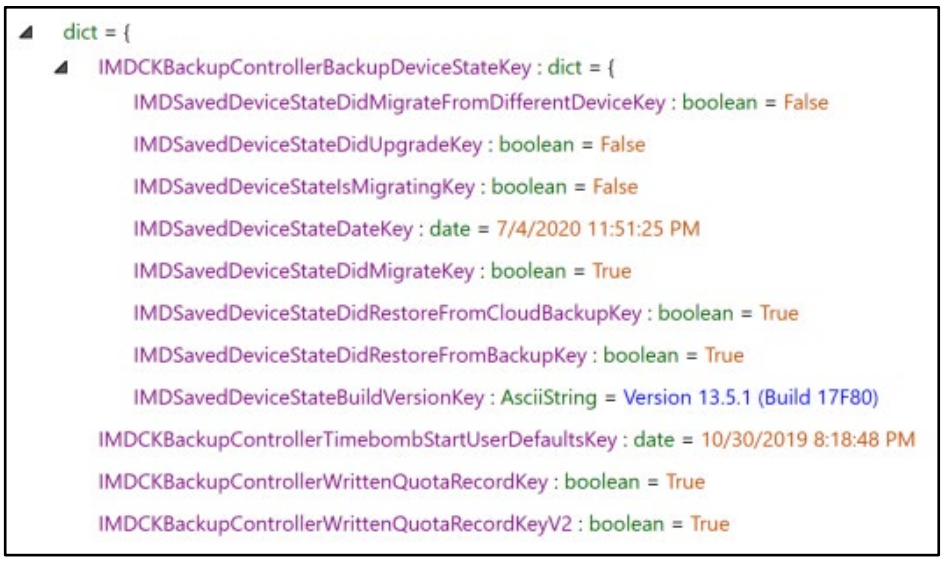


Figure 8 - A screenshot of the "com.apple.mobileSMS.plist" file from the August 21, 2020 iTunes backup of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Text Message Database

On an iPhone, the built-in application for text messaging is the "Messages" application. Data for the "Messages" application is stored in a SQLite database file named "sms.db," typically found in the "/private/var/mobile/Library/SMS" folder. Within this database, text messaging data is split across multiple database "tables." The two main tables considered in this analysis were the "chat" table and the "message" table. The "chat" table contains records of conversation threads that occurred on the iPhone. The "message" table contains records of individual messages that can be grouped into the conversation threads listed in the "chat" table. The "message" table, among others, assigns a unique, auto-incrementing, primary key, named the "ROWID." This value starts at "1," and increments by 1 for each additional record added to the "message" table. When a text message associated with a specific ROWID is deleted from a phone, that row is removed from the "message" table and the ROWID is eliminated, but the remaining rows in the table retain their existing ROWID values. As a result, an analysis of the "message" table can identify gaps in the sequential numbering of "ROWID" values, which would represent missing/deleted text messages.

The ROWID in the "message" table is used to link messages with conversation threads in the "chat" table, as well as to link messages with information in other tables. Each conversation thread in the "chat" table is also assigned a unique and sequential "ROWID" used for linking with information in other tables.

The following graphics are intended to help demonstrate how information in the “message” table links up with information in the “chat” table. The first graphic shows an exemplary conversation in the Messages application as seen on an iPhone.

Figure 9 - A screenshot of an exemplary conversation in the Messages application

The next graphic shows how items in the “message” table link to a conversation thread in the “chat” table through an intermediary table named “chat_message_join.”

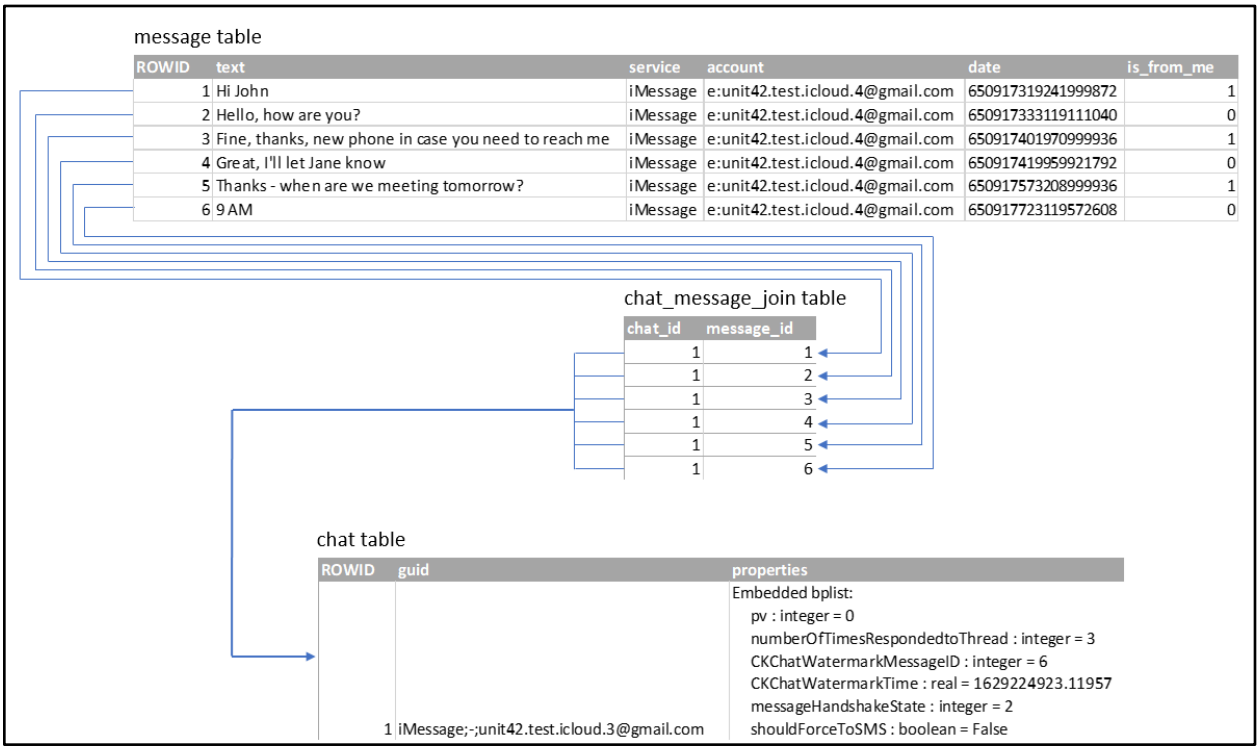


Figure 10 - A high level representation of select columns from three tables in the “sms.db” database based on the exemplary conversation shown above in Figure 9 (Time codes displayed are in UTC.)

In addition to text messages being stored locally on an iPhone in the “sms.db” file, text messages can also be stored in iCloud in two different ways.[10] First, a user can utilize the “Messages in iCloud” feature to synchronize messages to iCloud. Second, a user can store text messages in iCloud backups. However, only one of the iCloud storage methods may be used at a given time. Text messages are not stored in iCloud backups if the “Messages in iCloud” feature is enabled. Similarly, if the “Messages in iCloud” feature is disabled, then iCloud backups do contain text messages.

“Messages in iCloud” Synchronization Settings

On an iPhone, settings related to the “Messages in iCloud” feature are stored in a configuration file named “com.apple.madrid.plist.” The “com.apple.madrid.plist” file is typically located in the “/private/var/mobile/Library/Preferences” folder on an iPhone. The “CloudKitSyncingEnabled” key has a value of “True” or “False.” “True” indicates that text messages are configured to synchronize to iCloud using the “Messages in iCloud” feature. “False” indicates that text messages are configured not to synchronize to iCloud using the “Messages in iCloud” feature. Furthermore, if “Messages in iCloud” is enabled, the “CloudKitInitialStartDate" key will have a value that reflects the date and time this feature was enabled.[11] When the “Messages in iCloud” feature is enabled, text messages are automatically synchronized to, and stored in, iCloud but are not included in any iCloud backups created while “Messages in iCloud” remains enabled.[12]

The following figure shows a limited preview of the contents of the “com.apple.madrid.plist” configuration file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), which was identified on Ms. Chen’s computer.

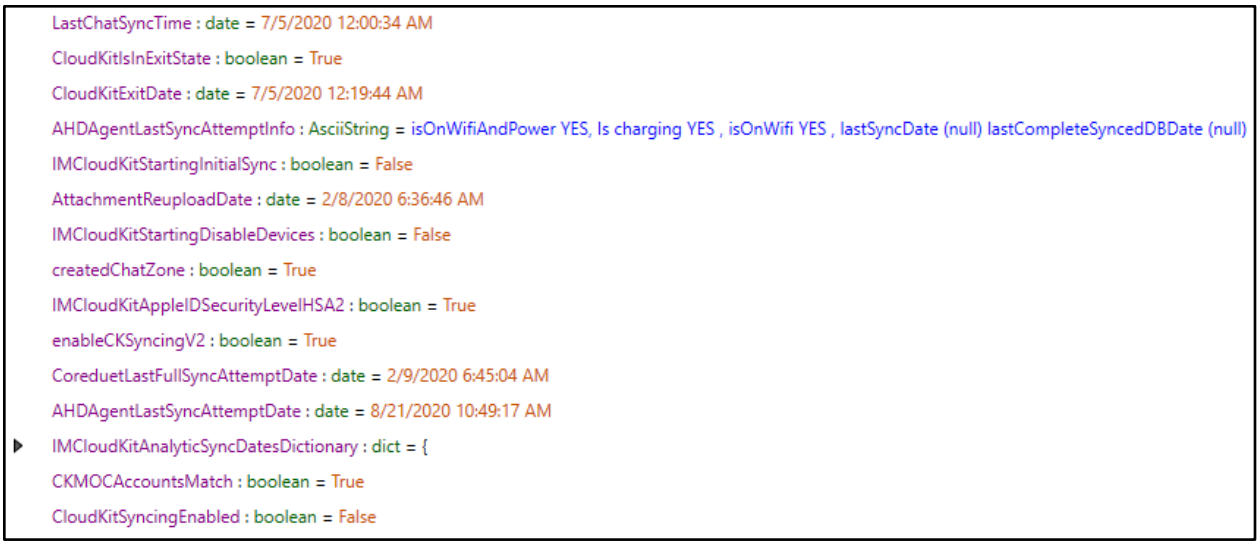


Figure 11 - A screenshot of a limited preview of the “com.apple.madrid.plist” file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

[10] Text messages stored in iCloud can include the traditional “SMS” text messages, as well as Apple proprietary iMessage text messages.

[11] The “CloudKitInitialStartDate” key will have a value associated with the date and time that “Messages in iCloud” was last enabled on the device and not the first time “Messages in iCloud” was enabled on the device if it was turned on and off and on again multiple times.

[12] Apple’s documentation in Footnote 2 of this page (https://support.apple.com/en-us/HT207428) confirms this to be accurate. The following page (https://support.apple.com/guide/icloud/messages-mm0de0d4528d/icloud) adds additional context.

Unit 42 is aware of two ways in which a user can choose to disable “Messages in iCloud,” neither of which affects the storage of text messages on the phone; just in iCloud. The “Messages” toggle can be turned off within the “iCloud” menu of the “Settings” application, or “Messages in iCloud” can be turned off via the “Disable & Delete” feature within “iCloud Storage.” Notably, turning off “Messages in iCloud” with the “Disable & Delete” feature causes two keys, named “CloudKitExitDate” and “CloudKitIsInExitState” to be created in the “com.apple.madrid.plist” file. The key “CloudKitIsInExitState” will have a value of “True” if the “Disable & Delete” function was used. The key “CloudKitExitDate” will have a value representing the date and time the “Disable & Delete” function was used. These two keys are created only when using “Disable & Delete”; they are not created when turning off “Messages in iCloud” via the toggle in the “iCloud” menu. Neither of these functions delete messages from an iPhone, but rather stop the synchronization of messages to iCloud and for the “Disable & Delete” function, also delete the synchronized messages from iCloud after 30 days. A screenshot of the steps taken to disable “Messages in iCloud,” as it appears on an iPhone, is shown in the following figure.

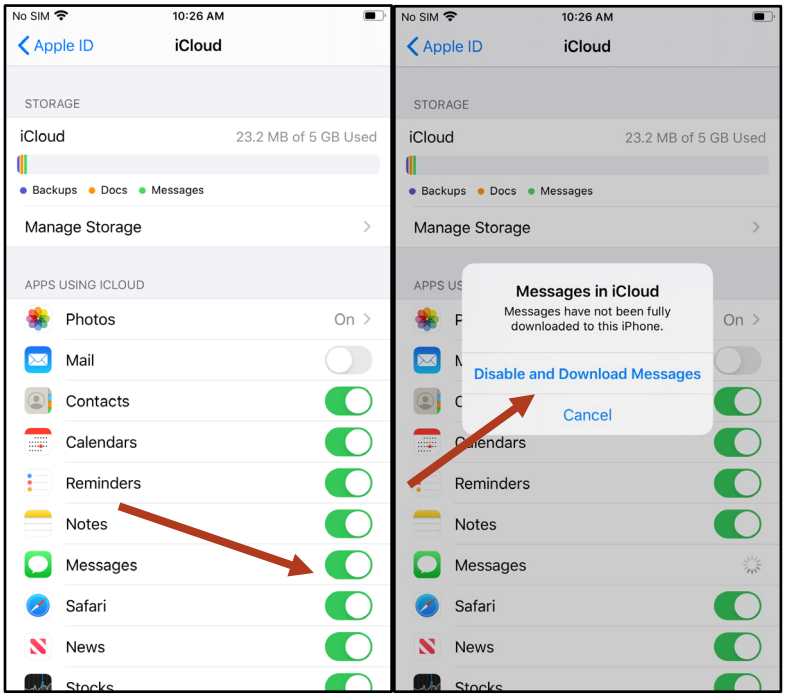


Figure 12 - Screenshots of the “iCloud” menu. The “Messages in iCloud” feature can be disabled by sliding the “Messages” toggle in the “iCloud” menu (shown above with a red arrow) to the left and selecting “Disable and Download Messages”

The steps to “Disable & Delete” “Messages in iCloud” are shown in the following screenshots.

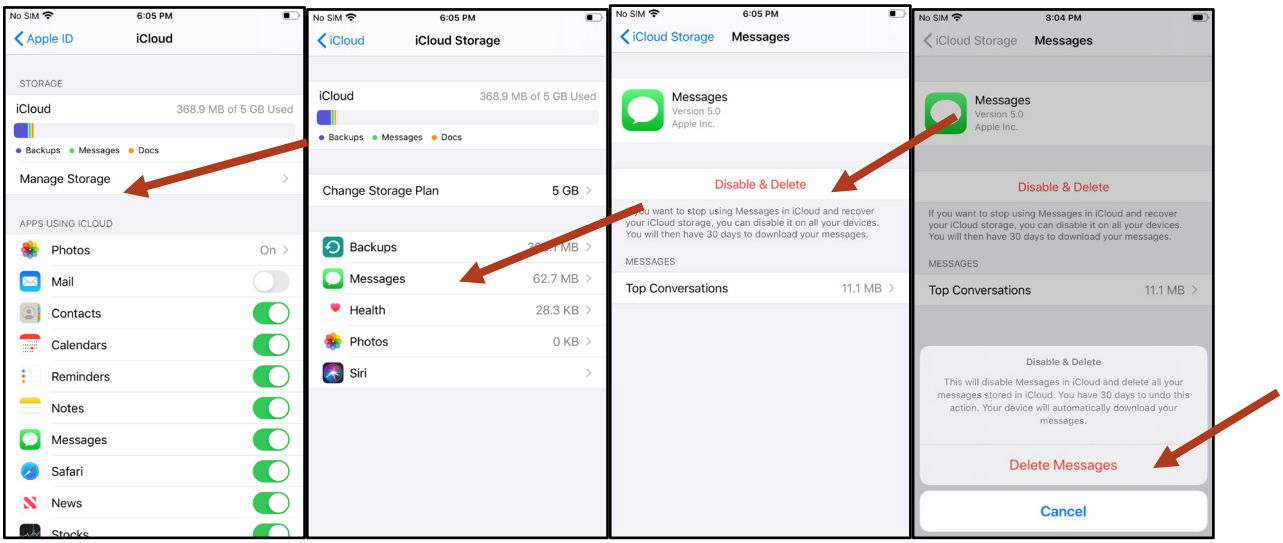


Figure 13 - Screenshots of the “iCloud,” “iCloud Storage,” and “Messages” menus. “Messages in iCloud” can be disabled by clicking “Disable & Delete” on the “Messages” menu

iCloud Backup Settings

On an iPhone, settings related to iCloud backups are stored in a configuration file named “com.apple.mobile.ldbackup.plist.” The “com.apple.mobile.ldbackup.plist” file is typically located in the “/private/var/mobile/Library/Preferences” folder. The “CloudBackupEnabled” key has a value of “True” to indicate that the iPhone was configured to automatically backup to iCloud. “False” indicates that the iPhone was configured not to backup to iCloud. In this same configuration file, the “LastCloudBackupDate,” if it exists, has a value that reflects the date and time of the last iCloud backup. If this key does not exist, an iCloud backup of this device has not previously been performed.

If iCloud backup is enabled, then the iPhone will automatically backup to iCloud when it is connected to a power source, connected to a Wi-Fi network, and the screen is locked. A user can also navigate to a menu option to manually initiate a backup at any time. If iCloud backup is disabled, then the iPhone will not automatically backup, and there will not be an option to manually initiate a backup.

When iCloud backups are performed, the contents of the backups are stored in iCloud on Apple’s servers. If a device that was previously backing up to iCloud stops backing up, the existing backups in iCloud will be held for 180 days. After 180 days, iCloud backups of a device that is no longer backing up to iCloud will be automatically deleted by Apple.[13]

The figure below shows the contents of the “com.apple.mobile.ldbackup.plist” configuration file from the July 7, 2021, full file system data extraction of the iPhone 8 Plus (Verizon). The date values in this configuration file are stored in Apple Absolute Time.[14]

[13] For more information, see https://support.apple.com/en-us/HT207428 and https://www.apple.com/legal/internet-services/icloud/en/terms.html Section II, C (Backup).

[14] Apple Absolute time uses integers that represent the number of seconds since January 1, 2001, at 00:00:00 UTC to store dates/times. (https://developer.apple.com/documentation/corefoundation/1543542-cfabsolutetimegetcurrent).

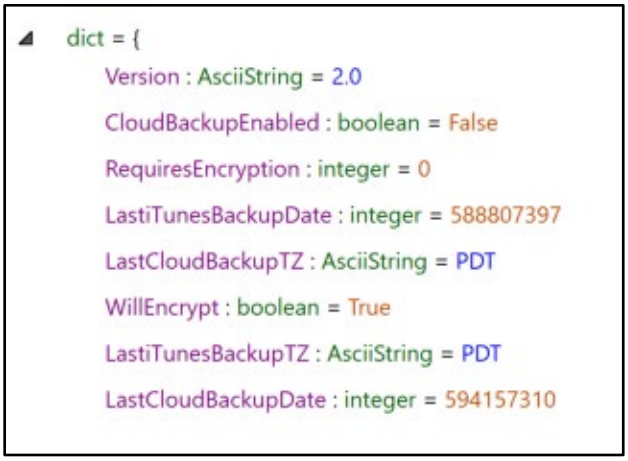


Figure 14 - A screenshot of the "com.apple.mobile.ldbackup.plist" file from the July 7, 2021 full file system data extraction of the iPhone 8 Plus (Verizon) as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Time codes displayed are in UTC.)

A SQLite database, named "cloudkit_cache.db," records data related to recent iCloud backups. This database is typically located in the "/private/var/root/Library/Caches/Backup" folder on an iPhone. This database contains a table, named "Snapshots," which records recent iCloud backups of a given device. Each "Snapshot" represents an iCloud backup. The "created" date listed for each snapshot records the date and time that the backup was taken.[15]

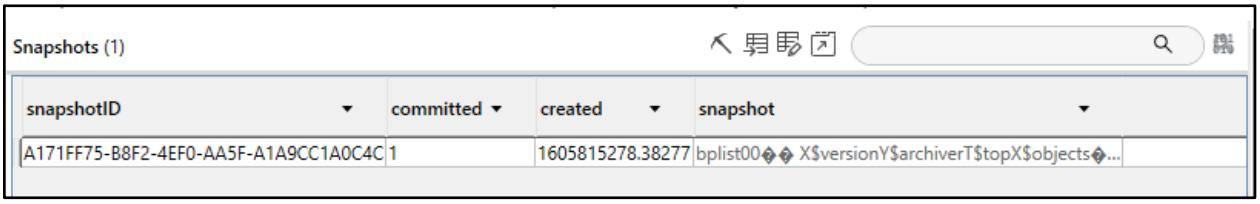


Figure 15 - A screenshot of an entry in the "Snapshots" table of the database "cloudkit_cache.db" from the July 8, 2021, full file system data extraction of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.48.1.3) (Times codes displayed are in UTC)

The "snapshot" field contains configuration information about the iCloud backup, as shown in part in the following figure. The complete set of configuration information is very lengthy, so a partial screenshot was captured to show many of the more relevant key/value pairs.

[15] This date is in UNIX epoch time, which is represented in seconds since January 1, 1970, 00:00:00 UTC.

Figure 16 - A limited screenshot of the binary plist configuration data stored in the "snapshot" field, from the "Snapshots" table of the database "cloudkit_cache.db" from the July 8, 2021, full file system data extraction of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.48.1.3) (Times displayed are in UTC.)

Text Message Retention Settings

On an iPhone running any of the versions of Apple's iOS operating system in use on Mayor Durkan's or Chief Best's multiple iPhones examined by Unit 42, the Message History settings are stored in a configuration file named "com.apple.MobileSMS.plist." Unit 42 has confirmed through testing on test devices that the default Message History setting for how long to "Keep Messages" is "Forever."

Once the Message History settings controlling how long to "Keep Messages" is changed, the key "KeepMessageForDays" is written to the configuration file "com.apple.MobileSMS.plist." This key will have a numeric value of "365" to keep messages for one year, a value of "30" to keep messages for 30 days, or a value of "0" to keep messages "Forever." On a newly setup iPhone or on an iPhone that has never had this setting changed, the key is not present in the configuration file, which also means that the default option of keeping messages "Forever" is active. The key "KeepMessageForDays" is set to "0" when the option has been set to something other than keeping messages forever, and later, the setting has been changed back to keep forever. Enabling "Messages in iCloud" or using the Messages "Disable & Delete" function also explicitly sets the Message History settings to "Keep Messages" "Forever" which, in turn, creates the key. While it is possible to determine if the Message history setting "Keep Messages" has been changed, iPhones do not track, log, or otherwise document the timing of when such changes are made.

Another key, “KeepMessagesVersionID,” is added to the configuration file “com.apple.MobileSMS.plist,” when a user updates the Message History settings. The “KeepMessagesVersionID” contains a numeric value that increments each time the Message History setting is updated. This key is not present on a newly setup iPhone or on an iPhone that has never had the Message History settings controlling how long to “Keep Messages” changed from the default option of keeping messages “Forever.” Each time the “Keep Messages” setting is changed, this “KeepMessagesVersionID” numeric value increments by 1, as confirmed by testing performed by Unit 42 on test devices. In addition to changing the Message History setting manually, enabling “Messages in iCloud” or using the Messages “Disable & Delete” function to disable and delete “Messages in iCloud” increments the “KeepMessagesVersionID” numeric value by 1 as they both set Message History to “Forever” even if “KeepMessageForDays” is already set to “0.” That is, even if Message History is set to “Forever,” enabling “Messages in iCloud” or using “Disable & Delete” will increment the “KeepMessagesVersionID” by 1. To date, Unit 42 is not aware of any other changes to other settings related to Messages that will increment this number. Should Unit 42 later learn of any such settings it reserves the right to supplement or amend this report.

The figure below shows a limited preview of the contents of the “com.apple.MobileSMS.plist” configuration file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), stored on Ms. Chen’s computer.

Figure 17 - A screenshot of a limited preview of the “com.apple.MobileSMS.plist” file from the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) as viewed in Cellebrite Physical Analyzer (v7.47.0.49)

Manual Deletion of Messages

In the “Messages” application, when a user manually deletes one or more individual messages, the corresponding entries are deleted from the “message” table, but a record of the conversation will remain in the “chat” table even if the individual messages deleted are the last messages in the conversation thread. The deletion of entries from the “message” table, (but not the “chat” table) also occurs if a user opens a

conversation thread and manually chooses the “Delete All” option to delete all messages in that conversation thread. The corresponding entry in the “chat” table will remain in this scenario as well.

The following figure shows screenshots of the process to manually delete one, more than one, or all messages within a conversation thread. As depicted by the red arrows in the following figure, to delete one or more messages, one would open the corresponding conversation thread and then press and hold (also called “long press”) on any one of the individual messages (Figure 18a). That will bring up the reactions and menu, where one can choose “More” to bring up options to forward or delete messages (Figure 18b). One can then use the check boxes to select one or more messages, click the “Trash Can” in the bottom left corner (Figure 18c), and then select “Delete Message(s)” (Figure 18d). Alternatively, to delete all messages in this conversation thread, one would select the “More” menu option followed by “Delete All” in the upper left corner (Figure 18e) and then select “Delete Conversation” (Figure 18f). This process will delete each selected message, up to all messages within the given conversation thread, by deleting the associated entries from the “message” table but will not delete any entries from the “chat” table.

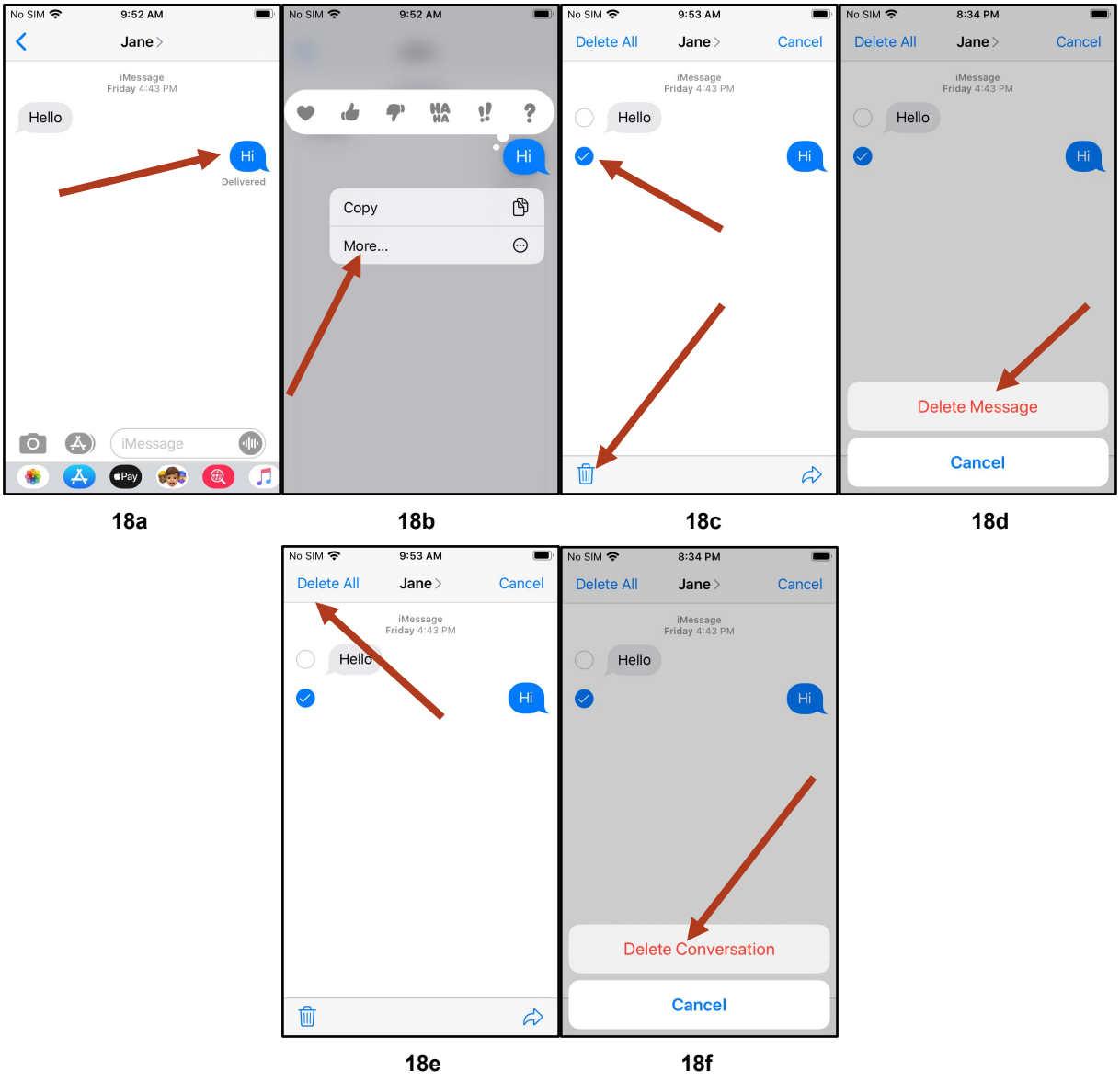


Figure 18 - Manual deletion of one or more text messages

However, when a user manually deletes an entire conversation thread, the corresponding entry is deleted from the “chat” table, and all associated messages are deleted from the “message” table.

The following figure shows screenshots of the process to manually delete a conversation thread. As depicted by the red arrows in the following figure, to delete a conversation thread, one would press and swipe left on the corresponding conversation thread. Then, one would choose “Delete” from the menu that is revealed for that conversation thread and then select “Delete” on the subsequent prompt. This process will delete the selected conversation thread, including all associated messages, by deleting the associated entries from the “message” table as well as the “chat” table.

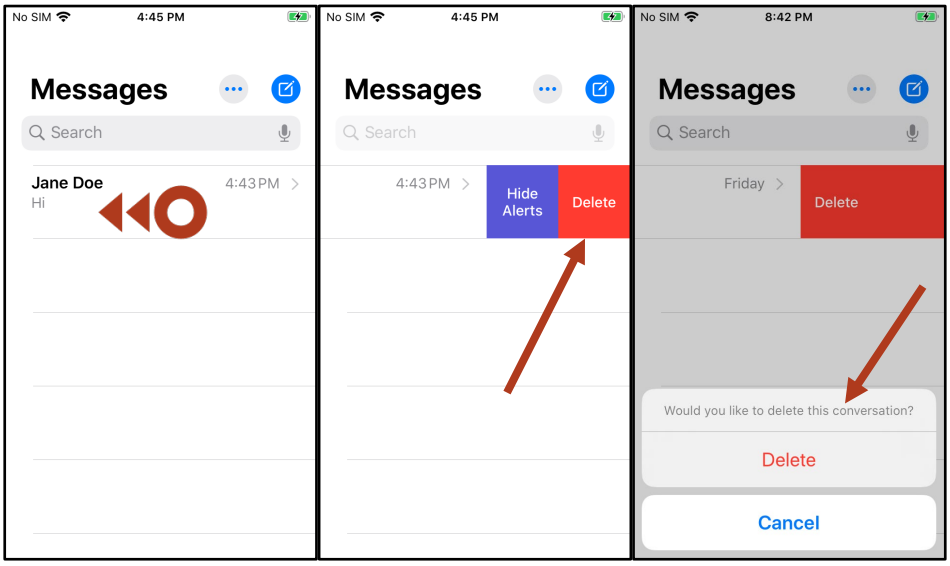


Figure 19 - Manual deletion of a conversation

Deletion of Messages Based on “Message History” Settings

When the Message History setting “Keep Messages” is changed to keep 30 days or one year of messages, the entries in the “message” table older than the selected retention period are deleted.[16] As time progresses, any messages older than the configured time to keep messages are subsequently deleted, and their entries are removed from the “message” table. This setting not only removes older messages beyond the retention threshold initially when the setting is configured, but also removes any messages on a nightly, rolling basis when they exceed the configured retention period, until the setting is changed to a longer retention period. Changing the setting to “Keep Messages” “Forever” will end the deletion process altogether.

Unit 42 has confirmed through testing on test devices that, if the date of every message in a conversation thread exceeds the configured time to keep messages, then the database entries for all messages from that conversation thread are deleted from the “message” table. The associated entries in the “chat” table, however, are not automatically removed, even if all messages associated with that conversation thread are deleted for exceeding the configured retention period. Therefore, the “chat” table will retain records of conversation threads that are older than the message retention settings. The actual text of the conversations will not be retained, however, because message contents are stored in the “message” table. This pattern is also seen with the manual use of the “Delete All” option within a conversation thread but differs from activity associated with the manual deletion of conversation threads, in which case the entries from both the “message” and “chat” tables would be deleted.

[16] For more information, see https://support.apple.com/en-us/HT201287.

Thus, messages deleted automatically by the Message History settings leave behind entries in the "chat" table, while manually deleted conversation threads do not leave behind these records. The presence of entries in the "chat" table to which no messages are associated may indicate that those deletions occurred automatically as a result of the Message History settings rather than representing manual deletions performed by a user.[17]

The Message History settings only provide three options that may be configured on an iPhone. The options are to "Keep Messages" for "30 Days," for "1 Year," or "Forever." Having a number of entries in the "chat" table with no associated messages is consistent with the "Keep Messages" setting having been configured to either "30 Days" or "1 Year" at some point in time.

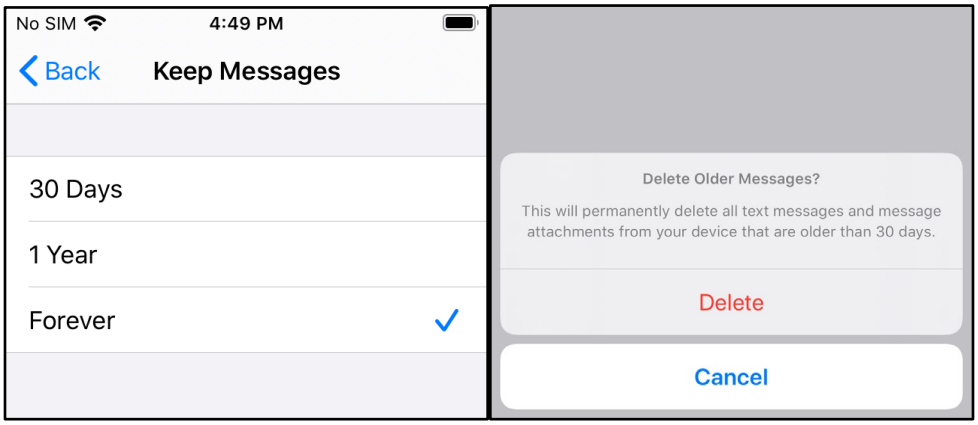


Figure 20 - A screenshot of the "Keep Messages" menu options and the message displayed when changing from the "Forever" option to the "30 Days" option

Resetting an iPhone

When an iPhone is "reset to factory defaults" using the "Erase All Content and Settings" option, all data, content, settings, and configurations are erased from the iPhone.[18] No information present before the factory reset occurred will remain on the iPhone. Multiple forensic artifacts are created during the process, which can be used to identify when the factory reset occurred. In particular, a file named ".obliterated" will be created, typically in the "/private/var/root" folder, available only in a "full filesystem" extraction of data from an iPhone. The creation date and time of this file reflects the first time that the iPhone booted up after the factory reset occurred. However, because this first boot happens automatically once the factory reset process completes on an iPhone, this date also can be associated with the factory reset process. Additional artifacts can also help establish when a factory reset occurred, such as the creation of certain databases and system files, as well as entries in certain log files.

[17] Entries in the "chat" table to which no messages are associated may also indicate manual deletion of all messages within each conversation thread using the "Delete All" function or by individually selecting each message and deleting them. For these situations—entries in the "chat" table for which there are no associated messages—there is typically no forensic artifact, log, or record indicating whether the messages were deleted manually or because of the Message History settings. When a large number of "chat" table entries are not associated with any messages, one could infer that it was the result of a Message History setting, because to complete that process through manual deletion would entail a systematic, lengthy, and burdensome process by someone with access to the iPhone. Conversely, when a small number of "chat" table entries are not associated with any record in the "messages" table, it may be difficult to infer the deletion method employed.

[18] For more information, see https://support.apple.com/guide/iphone/erase-iphone-iph7a2a9399b/14.0/ios/14.0.

Mayor Durkan's iPhone 8 Plus (Verizon) Analysis and Findings

iPhone Setup Information

In both the August 29, 2019, backup and the full file system collection representing this iPhone's configuration as of October 30, 2019, the configuration file "com.apple.MobileBackup.plist" contains the "RestoreDate" key with a value that represents April 10, 2018, at 17:13:32. Additionally, the "WasCloudRestore" key in the same configuration file had a value of "True," indicating that the iPhone 8 Plus (Verizon) was set up by a restoration from an iCloud backup on April 10, 2018, at 17:13:32.

Text Message Retention Settings

In the August 29, 2019, backup, the configuration file "com.apple.MobileSMS.plist" does not contain the keys "KeepMessageForDays" or "KeepMessagesVersionID." The absence of these keys indicates that this iPhone was configured to keep its messages forever and that at no point in time was this setting changed to any other Message History value between the time that the phone was provisioned and the time the backup was taken.

In the full file system collection performed by Unit 42 on July 7, 2021, the configuration file "com.apple.MobileSMS.plist" contained the "KeepMessageForDays" key and had a value set to "0," which means that messages will be kept forever. The presence of this key indicates that the setting was updated at one point in time. The "KeepMessagesVersionID" key has a value set to "1," which indicates that this setting was changed just one time between August 29, 2019, and on October 30, 2019, when the device was decommissioned and user activity on the device ceased. Taken together, these artifacts indicate that the "KeepMessages" setting was set to "Forever" sometime between August 29, 2019, and October 30, 2019. As explained below, "Messages in iCloud" was enabled on this phone on October 30, 2019, at 19:40:35, which would have set "KeepMessages" to "Forever" (even though "KeepMessages" was already set to "Forever") and would account for the existence and values of the "KeepMessageForDays" and "KeepMessagesVersionID" keys.

Analysis showed that this iPhone was set to "KeepMessages" "Forever" at all times the phone was in use.

Synchronizing Messages to iCloud Settings

In the August 29, 2019, backup, the configuration file "com.apple.madrid.plist" contains the "CloudKitSyncingEnabled" key with a value of "False," indicating that text messages were not configured to synchronize with iCloud using the "Messages in iCloud" feature, at the time of the backup.

In the full file system collection performed by Unit 42, the configuration file "com.apple.madrid.plist" contained the "CloudKitSyncingEnabled" key and had a value set to "True," indicating that text messages were configured to synchronize with iCloud using the "Messages in iCloud" feature. Specifically, the change from "False" to "True" must have occurred on October 30, 2019, at 19:40:35 when "Messages in iCloud" was enabled based on the date of the "CloudKitInitialStartDate" key. This explains why the "KeepMessagesVersionID" value was set to "1," and the KeepMessagesForDays to "0," because, as explained above, when an iPhone is initially set up, the "KeepMessagesForDays" key is initially nonexistent. A value of "0" in that key and a "KeepMessagesVersionID" of "1" is consistent with turning on the "Messages in iCloud" feature, which would populate the "KeepMessagesforDays" key with a "0" (i.e., retaining messages "Forever"), and increment the "KeepMessagesVersionID" by 1.

Backup Setting

In both the August 29, 2019, backup and the full file system collection of the iPhone 8 Plus (Verizon), the configuration file "com.apple.mobile.ldbackup.plist" contains the "CloudBackupEnabled" key and has a value set to "False," indicating that the device was not configured to automatically backup to iCloud at the time the collections were performed.

In the August 29, 2019, backup, the configuration file "com.apple.mobile.ldbackup.plist" contains the "LastCloudBackupDate" key with a value representing the date August 29, 2019, at 05:51:20. Because this iCloud backup occurred earlier the same day the device was backed up to iTunes, Unit 42 infers that iCloud backup was disabled that day, as backups to iCloud can only occur with the setting enabled.

In the full file system collection, the "LastCloudBackupDate" value reflected the date October 30, 2019, at 19:41:50, indicating that another iCloud backup had occurred. This October 30, 2019, iCloud backup also suggests that iCloud backup was enabled, the backup was taken, and then iCloud backup was disabled again, as backups to iCloud can only occur with the setting enabled.

On November 16, 2020, Unit 42 inspected and preserved data from the iCloud account associated with this device and determined that no iCloud backups were available in the iCloud account. This is consistent with Apple's policy to delete iCloud backups for devices that have not backed up to iCloud in more than 180 days.[19]

The "LastiTunesBackupDate" key in the "com.apple.mobile.ldbackup.plist" file contains values representing the last date on which an iTunes backup was created. In the August 29, 2019, iTunes backup, this value represented the date May 24, 2019, at 22:56:38 and, in the full file system collection performed by Unit 42, the value was August 29, 2019, at 21:36:37, which was the date and time of the August 29, 2019, iTunes backup identified on Ms. Chen's computer.

Text/Chat Message Analysis

The August 29, 2019, backup contains 3,643 active text messages from November 18, 2017, to August 29, 2019 (the date of the backup). The full file system collection contains 3,845 active text messages from November 18, 2017, to October 30, 2019, the date the device was taken out of use. The full file system collection captured unique text messages between August 29, 2019, and October 30, 2019, that had not been found in other sources.

Mayor Durkan's iPhone 8 Plus (FirstNet) Analysis and Findings

Unit 42 reviewed the three different collections of the iPhone 8 Plus (FirstNet) and identified that no text messages or historical configurations were recoverable from this device. This is consistent with Unit 42's understanding that the City's IT personnel reset the device to factory defaults after the phone was decommissioned.

On July 9, 2020, the iPhone 8 Plus (FirstNet) was used to configure the iPhone 11 (FirstNet) using the "Quick Start" method, and, as a result, some of the artifacts on the iPhone 11 (FirstNet) were derived or transferred from the iPhone 8 Plus (FirstNet). The findings mentioned below are primarily from iPhone 11 (FirstNet) data sources that include information attributable to the iPhone 8 Plus (FirstNet).

iPhone Setup Information

Unit 42 understands that the iPhone 8 Plus (FirstNet) was in use from October 30, 2019, until July 9, 2020. Because the data on the iPhone 8 Plus (FirstNet) was transferred to the iPhone 11 (FirstNet) on July 9, 2020, and the iPhone 8 Plus (FirstNet) was subsequently reset to factory defaults, Unit 42 could not analyze this phone directly to determine how it had originally been set up.

To determine how the iPhone 8 Plus (FirstNet) was set up, Unit 42 analyzed the full file system extractions of the iPhone 8 Plus (Verizon) and the iPhone 11 (FirstNet). Analysis of data extractions from these iPhone devices, used just before and after the iPhone 8 Plus (FirstNet), respectively, showed that data from the iPhone 8 Plus (Verizon) was present on the iPhone 8 Plus (FirstNet), which was then transferred to the iPhone 11 (FirstNet). Specifically, the "ZLIVEUSAGE" and "ZPROCESS" tables in the DataUsage.sqlite database on the iPhone 11 (FirstNet) contained entries with dates prior to October 30, 2019, that matched entries in the same tables and database from the iPhone 8 Plus (Verizon). Because the iPhone 11 (FirstNet)

[19] For more information, see https://www.apple.com/legal/internet-services/icloud/en/terms.html.

was set up with the "Quick Start" method from the iPhone 8 Plus (FirstNet), and because the DataUsage.sqlite database does not synchronize with iCloud, this demonstrates that data from the iPhone 8 Plus (Verizon) was indeed transferred to the iPhone 8 Plus (FirstNet) as opposed to being present simply because the same iCloud account was signed in on both devices. These findings are consistent with Unit 42's understanding that the iPhone 8 Plus (FirstNet) was set up with the data from the iPhone 8 Plus (Verizon). Furthermore, based on the "timestamp" and "data" columns in the "keybag" table from multiple databases named backup.sqlite3 found in subfolders under the "/private/var/root/Library/Application Support/com.apple.sbd/EC5F4ACF-D770-43DD-961B-808BD8C56F2C" directory on the iPhone 8 Plus (Verizon), the iPhone 8 Plus (FirstNet) was associated with Mayor Durkan's iCloud account around October 30, 2019, at 20:09:41. This is roughly 30 minutes after the last iCloud backup was created on the iPhone 8 Plus (Verizon) on October 30, 2019, at 19:41:50. This information is consistent with the iPhone 8 Plus (FirstNet) having likely been set up by restoring the iCloud backup of the iPhone 8 Plus (Verizon).

Restore from iCloud on July 4, 2020

Unit 42 understands that the iPhone 8 Plus (FirstNet) was submerged in salt water on July 4, 2020, and, as a result, the phone was ultimately restored from an iCloud backup of itself on that date. As described below, the forensic data is consistent with the phone having been restored from an iCloud backup.[20]

In the August 21, 2020, iTunes backup and October 15, 2020, forensic extraction of the iPhone 11 (FirstNet), the configuration file "com.apple.mobileSMS.plist" contains multiple keys related to "Messages in iCloud," including "IMDSavedDeviceStateDidRestoreFromCloudBackupKey," "IMDSavedDeviceStateDidMigrateFromDifferentDeviceKey," and "IMDSavedDeviceStateDateKey." The "IMDSavedDeviceStateDidRestoreFromCloudBackupKey" key has a value set to "True." The "IMDSavedDeviceStateDidMigrateFromDifferentDeviceKey" has a value set to "False." The "IMDSavedDeviceStateDateKey" key has a value set to 7/4/2020 23:51:25.

The combination of these keys and values are consistent with the iPhone 8 Plus (FirstNet) being restored from an iCloud backup of itself on July 4, 2020, at 23:51:25 UTC (16:51:25 PDT) in which "Messages in iCloud" is enabled. Other more commonly used artifacts that could show that an iPhone had been restored from iCloud were not available because of the subsequent transfer of data to the iPhone 11 (FirstNet). However, there are numerous core system files, databases, and log files that contain the July 4, 2020, date and further support that the iPhone 8 Plus (FirstNet) was restored on this date.

There are indications that the iCloud backup of the iPhone 8 Plus (FirstNet) used for the restore on July 4, 2020, was taken in early-to-mid February 2020.

On the iPhone 11 (FirstNet), Unit 42 identified several logs and a database with regularly occurring entries dated up to and around February 9, 2020, followed by a gap in entries until July 4, 2020. One example is the "DataUsage.sqlite" database located in the "/private/var/wireless/Library/Databases" folder. Two tables in this database, "ZLIVEUSAGE" and "ZPROCESS," collectively record network metrics associated with different processes on the iPhone. In the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), the "ZLIVEUSAGE" table has 1,116 total entries that all include a "ZTIMESTAMP" column with numbers representing dates between November 17, 2017, and August 21, 2020. Among those entries, there are 596 entries associated with dates between November 17, 2017, at 00:49:01 and February 6, 2020, at 10:33:56. There is then a gap until July 4, 2020, at 23:51:54. Similarly, the "ZPROCESS" table has 368 total entries that all include a "ZTIMESTAMP" column with numbers representing dates between November 11, 2017, and August 21, 2020. Among those entries, there are 255 entries associated with dates between November 17, 2017, at 00:28:31 and February 9, 2020, at 06:57:30. There is then a gap until July 8, 2020, at 23:38:32.

Based on analysis of the exemplary database described above, as well as other log files from the iPhone 11 (FirstNet), there are indications that an iCloud backup of the iPhone 8 Plus (FirstNet) was taken in early-to-mid February 2020. After this early-to-mid February 2020 iCloud backup, the iPhone 8 Plus (FirstNet)

[20] Mayor Durkan 12/8/2021 Dep. Tr. at 255:7-256:17.

appears to have stopped backing up to iCloud. This is based on the fact that Apple only retains a very limited number of backups and an iPhone that was continuing to back up on a regular basis would have overwritten a backup from early-to-mid February 2020 by July 4, 2020, if the iPhone had continued to backup.

According to Apple's policy regarding iCloud backups, "If a device has not backed up to iCloud for a period of one hundred and eighty (180) days, Apple reserves the right to delete any backups associated with that device."[21] Because it is our experience that Apple deletes backups as allowed by this policy, i.e., at or around 180 days, we conclude that the early-to-mid February 2020 backup from the iPhone 8 Plus (FirstNet), was available for 180 days (i.e., until early-to-mid August 2020) and, therefore, was available to restore on July 4, 2020, but not available to restore after early-to-mid August 2020 (or in November 2020, when Unit 42 examined the relevant iCloud account for any iCloud backups).

Text Message Retention Settings

In the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), the configuration file "com.apple.MobileSMS.plist" contains the "KeepMessageForDays" key and has a value set to "0," which indicates that messages will be kept forever.

The "KeepMessagesVersionID" key has a value set to "4," which is consistent with the text message retention setting having been changed three times between October 30, 2019, (the date the iPhone 8 Plus (Verizon) was decommissioned and the "KeepMessagesVersionID" key had a value of "1") and August 21, 2020.

The "KeepMessageForDays" and "KeepMessagesVersionID" keys are retained when one iPhone is backed up and restored to another or transferred using the "Quick Start" method. Therefore, Unit 42 infers that the iPhone 8 Plus (FirstNet) started with the "KeepMessagesVersionID" key having a value of "1," inherited from the previous iPhone, the iPhone 8 Plus (Verizon).

After the iPhone 8 Plus (FirstNet) was restored from an iCloud backup on July 4, 2020, as discussed above, artifacts on the iPhone 8 Plus (FirstNet) indicate that the "Messages" "Disable & Delete" function in the iCloud Storage settings menu was used, also on July 4, 2020 PDT, as more fully described below. This "Messages" "Disable & Delete" function, among other things, sets "KeepMessages" to "Forever" (even if "KeepMessages" was already set to "Forever") thus incrementing the "KeepMessagesVersionID" key. Assuming the "KeepMessagesVersionID" key had not changed before this time, this action would have incremented the "KeepMessagesVersionID" key from a value of "1" to "2."

Further analysis based on forensic artifacts and testing is provided in the "Accounting for changes to iPhone Message History" section in this report because we cannot determine from the forensic artifacts or testing whether the changes described were made to the iPhone 8 Plus (FirstNet) or the iPhone 11 (FirstNet).

Synchronizing Messages to iCloud Settings

Based on the forensic artifacts from the iPhone 11 (FirstNet) device, Unit 42 determined that "Messages in iCloud" was enabled on the iPhone 8 Plus (FirstNet) before the "Disable & Delete" function for "Messages" in "iCloud Storage" was used on July 5, 2020, at 00:19:44 UTC (July 4, 2020, 17:19:44 PDT). Based on artifacts in the "com.apple.mobileSMS.plist" configuration file, as discussed above, Unit 42 inferred when and how the iPhone 8 Plus (FirstNet) was restored on July 4, 2020. The existence of these keys in the "com.apple.mobileSMS.plist" also confirm that "Messages in iCloud" was enabled in the iCloud backup that was used for the restore.

Therefore, Unit 42 infers that as of early-to-mid February 2020, when the iCloud backup that was later restored had been taken, "Messages in iCloud" was enabled on the iPhone 8 Plus (FirstNet).

[21] For more information, see https://www.apple.com/legal/internet-services/icloud/en/terms.html.

Because the iPhone was restored on July 4, 2020, from an iCloud backup that Unit 42 infers had "Messages in iCloud" enabled, Unit 42 found that the unique ROWID values in the "message" table of the iPhone Message's application database, "sms.db," were renumbered and reordered. As described previously in this report, each successive message sent or received by the device is assigned a unique integer as the ROWID, which is incremented one higher than the previous message. Therefore, newer messages have sequentially higher ROWIDs. When an iCloud backup is restored with "Messages in iCloud" enabled, however, the messages are synchronized down to the iPhone from iCloud beginning in reverse order (i.e., the newest message is assigned the smallest ROWID and the oldest message receives the highest ROWID). Although this process occurred on the iPhone 8 Plus (FirstNet), Unit 42 derived this finding by examining the "sms.db" database on the iPhone 11 (FirstNet), which was set up using data transferred from the iPhone 8 Plus (FirstNet). These artifacts indicate that approximately 5,911 messages were synchronized from iCloud onto the iPhone 8 Plus (FirstNet) when it was restored on July 4, 2020, the majority of which Unit 42 believes are separately available from the iPhone 8 Plus (Verizon).

This means that as of July 4, 2020, before the iPhone 8 Plus (FirstNet) was submerged, "Messages in iCloud" was enabled on the iPhone 8 Plus (FirstNet), because text messages from that time frame could only be synchronized with the iPhone 8 Plus (FirstNet) after the restore process if they had first been synchronized with iCloud beforehand.

Also, when the iPhone 8 Plus (FirstNet) was restored from an iCloud backup on July 4, 2020, "Messages in iCloud" remained enabled at that time because this setting is part of the configuration that was restored onto the device.

Given the number of messages added to the phone during the initial synchronization with iCloud, the date range of the messages synchronized was likely the full time frame for which Mayor Durkan possessed City provided mobile phones, from November 2017 to July 4, 2020. This would also mean that the majority of these messages are also still available from the iPhone 8 Plus (Verizon).

The "com.apple.madrid.plist" configuration file on the iPhone 11 (FirstNet) contains a key, named "CloudKitExitDate," whose value represents the date July 5, 2020, at 00:19:44 UTC (July 4, 2020, at 17:19:44 PDT). Based on testing on test devices, Unit 42 determined that this date is associated with the use of the "Messages" "Disable & Delete" function in the "iCloud Storage" menu. The "Messages" "Disable & Delete" function would have caused the iPhone 8 Plus (FirstNet) to stop synchronizing messages to iCloud and set all messages stored in iCloud to be deleted from iCloud (but not from the iPhone itself) in 30 days, on August 4, 2020 UTC (August 3, 2020 PDT). Using the "Disable & Delete" function also sets the text message retention setting on the iPhone to "Forever" (even if it is already set to "Forever"), and, as a result, increments the "KeepMessagesVersionID" key in the "com.apple.MobileSMS.plist" configuration file by 1.

Unit 42 infers, then, that as of July 4, 2020, at 17:19:44 PDT, "Messages in iCloud" was disabled, and remained disabled for the rest of the time this phone was in use. When this iPhone's configuration and data were transferred to the iPhone 11 (FirstNet) through the "Quick Start" feature, the setting disabling "Messages in iCloud" was included in that transfer.

Backup Settings

Because the iPhone 8 Plus (FirstNet) was reset to factory defaults, Unit 42 could not determine exactly when the iPhone 8 Plus (FirstNet) was last backed up to iCloud. Unit 42 identified artifacts confirming that the iPhone 8 Plus (FirstNet) was restored on July 4, 2020 from an iCloud backup of itself taken in early-to-mid February 2020. Had more recent backups existed in iCloud, they would have overwritten the early-to-mid February 2020 backup. Therefore, iCloud backup functionality was likely disabled shortly after the iCloud backup was taken in early-to-mid February 2020.

In the August 21, 2020, and October 15, 2020 collections of the iPhone 11 (FirstNet), the configuration file "com.apple.mobile.ldbackup.plist" does not contain the "LastCloudBackupDate" key. Unit 42 confirmed through testing on test devices that the "LastCloudBackupDate" key does transfer from one phone to

another when a phone is set up using the "Quick Start" feature, but not when restoring a phone from an iCloud backup. From this testing, Unit 42 infers that had an iCloud backup been taken when the data from the iPhone 8 Plus (FirstNet) was transferred to the iPhone 11 (FirstNet), the "LastCloudBackupDate" key should have been created noting the date of that backup and the key should have transferred to the iPhone 11 (FirstNet). Unit 42 understands that the City IT team's customary practice when migrating a user in the Mayor's office from one phone to another using the "Quick Start" feature was to create an iCloud backup of the source phone prior to performing the migration. We have found no evidence that an iCloud backup of the iPhone 8 Plus (FirstNet) was taken just prior to transferring data to the iPhone 11 (FirstNet).

Because the iPhone 8 Plus (FirstNet) was reset to factory defaults after it was decommissioned, Unit 42 also could not determine if or when the iPhone 8 Plus (FirstNet) was backed up to a computer with iTunes, prior to it having been factory reset. The "LastiTunesBackupDate" from the "com.apple.mobile.ldbackup.plist" file on the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet) related to a backup of the iPhone 11 (FirstNet) and not the iPhone 8 Plus (FirstNet).

Because Ms. Chen's computer contained iTunes backups of the iPhone 8 Plus (Verizon) taken on August 29, 2019, and the iPhone 11 (FirstNet) taken on August 21, 2020, Unit 42 examined Ms. Chen's computer for evidence of any backups taken of the iPhone 8 Plus (FirstNet). Unit 42 searched for, but did not find, any backups of the iPhone 8 Plus (FirstNet), but did locate an Apple file named "iPodDevices.xml" in the folder path "C:\ProgramData\Apple Computer\iTunes\." The iPodDevices.xml file keeps a list of each Apple device connected, details about the device including the Serial Number, and a "Use Count" reflecting how many times each device was connected, among other things. Records existed in the iPodDevices.xml file for the iPhone 8 Plus (Verizon) and the iPhone 11 (FirstNet), but the file did not contain a record for the iPhone 8 Plus (FirstNet).

This indicates that the iPhone 8 Plus (FirstNet) was not connected or backed up to Ms. Chen's computer.

Text/Chat Message Analysis

The oldest text messages from the iPhone 11 (FirstNet) were dated June 25, 2020. Since the iPhone 11 (FirstNet) was not configured until July 9, 2020, it can be inferred that the text messages between June 25, 2020, and July 9, 2020, were stored on the iPhone 8 Plus (FirstNet), and transferred over on July 9, 2020, when the iPhone 8 Plus (FirstNet) was used to configure the iPhone 11 (FirstNet) through the "Quick Start" process.

It can also be inferred that because artifacts indicate approximately 5,911[22] messages were synchronized to the iPhone 8 Plus (FirstNet) as part of the July 4, 2020 restore process, the "30 Days" text message retention setting must have not been turned on prior to the iCloud restore when messages were added to the iPhone 8 Plus (FirstNet) through synchronization with iCloud. This is because the quantity of messages synchronized from iCloud after the restore, based on the average message volume observed, was far too large to represent only a 30-day period. If the "30 Day" setting had been enabled prior to the restoration and synchronization from iCloud, then only 30 days of messages would have been available to synchronize. The number of messages synchronized from iCloud indicates that the date range of the messages synchronized was likely the entire time frame for which Mayor Durkan possessed City-provided mobile phones, from November 2017 to July 4, 2020. From this information, Unit 42 infers that the "30 Day" Message History setting was set after the restoration and synchronization of messages from iCloud.

As discussed in more detail in the "Accounting for Changes to iPhone Message History," the "30 Days" text message retention must have been turned on after "Messages in iCloud" was disabled by the "Disable & Delete" function. Otherwise, the change would have resulted in a higher "KeepMessagesVersionID" than was found because "30 Days" would have to have been specified twice; once after the restore and before "Disable & Delete" and once again after "Disable & Delete" as "Disable & Delete" sets text message retention to "Forever." Furthermore, this hypothetical second configuration of the Message History settings

[22] Unit 42 believes the majority of these 5,911 messages are separately available from the iPhone 8 Plus (Verizon).

to “30 Days” could not be skipped because, in that scenario, the oldest text messages would have dated back to June 4, 2020, which they do not.

Additionally, when “Messages in iCloud” is enabled, several entries are created in the “sqlite_sequence” table of the Messages application database, “sms.db.” After “Messages in iCloud” is enabled, an entry named “sync_deleted_messages” is created and stores a running counter of the number of deleted messages that have been synchronized with iCloud. This number includes messages deleted by the Message History settings having been configured to keep messages for “30 Days” and manual deletions of text messages. Even if “Messages in iCloud” is later disabled, this value not only persists but will continue to be updated even though messages are no longer synchronizing with iCloud.

In the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), the value of the “sync_deleted_messages” counter is “5869.” This indicates that 5,869 messages, believed to date back to November 2017, were deleted between July 4, 2020, when the iPhone 8 Plus (FirstNet) was restored and this counter was reset to “0,” and August 21, 2020 (the date of the iTunes backup in which this copy of the “sms.db” file was captured).

Because the deleted messages are believed to date back to November 2017, a majority of the deleted messages separately exist on the iPhone 8 Plus (Verizon), from which 3,845 active text messages from November 18, 2017, to October 30, 2019 were identified.

Evidence of Factory Reset

Unit 42 understands that after the phone was decommissioned, a member of the City’s IT department factory reset the iPhone 8 Plus (FirstNet) in August 2020, as was the IT department’s customary practice. Unit 42 analyzed the iPhone 8 Plus (FirstNet) and confirmed that it had been reset and set up as described by the City “Information Security Engineer.” The iPhone 8 Plus (FirstNet) did not contain any recoverable text messages related to Mayor Durkan.

Mayor Durkan’s iPhone 11 (FirstNet) Analysis and Findings

iPhone Setup Information

In all four of the different collections from the iPhone 11 (FirstNet), the configuration file “com.apple.MobileBackup.plist” contains the “RestoreDate” key and has a value representing the date July 9, 2020, at 19:59:36, indicating that a restore occurred on July 9, 2020. Furthermore, the same configuration file shows that the iPhone 11 (FirstNet) was set up from an iPhone with the “SourceDeviceUDID” of “51d7744ec8caef13591bc3781180dfd37eb85455.” This is a unique identifier from the iPhone 8 Plus (FirstNet) phone and indicates the iPhone 11 (FirstNet) was set up via the “Quick Start” method from the iPhone 8 Plus (FirstNet).

Text Message Retention Settings

In all four collections of data from the iPhone 11 (FirstNet), the configuration file “com.apple.MobileSMS.plist” contains the keys “KeepMessageForDays” and “KeepMessagesVersionID.”

In each of these data sources, the “KeepMessageForDays” key has a value set to “0,” which indicates that messages will be kept forever.

In the August 21, 2020, backup and the October 15, 2020, collection, the “KeepMessagesVersionID” keys have a value of “4.” A value of “4” indicates that the Message History setting was updated four times.

The “KeepMessageForDays” and “KeepMessagesVersionID” keys are retained when one iPhone is backed up and restored to another or transferred using the “Quick Start” method. Therefore, Unit 42 inferred that the iPhone 11 (FirstNet) started with the “KeepMessageForDays” and “KeepMessagesVersionID” keys having values inherited from the previous iPhone, the iPhone 8 Plus (FirstNet).

In both of the collections performed by Unit 42, the “KeepMessageForDays” has a value of “0” and “KeepMessagesVersionID” has a value of “5,” which means the “Keep Messages” setting was updated between October 15, 2020, and November 19, 2020. On November 19, 2020, “Messages in iCloud” was enabled before the iPhone 11 (FirstNet) was provided to and preserved by Unit 42, which would set “KeepMessages” to “Forever” (even if “KeepMessages” was already set to “Forever”) and would increment the “KeepMessagesVersionID” from a value of “4” to “5.”

Further analysis based on forensic artifacts and testing is provided in the “Accounting for Changes to iPhone Message History” section in this report because we cannot determine from the forensic artifacts or testing whether the changes described were made to the iPhone 8 Plus (FirstNet) or the iPhone 11 (FirstNet).

Synchronizing Messages to iCloud Settings

In the August 21, 2020, backup and the October 15, 2020, collection, the configuration file “com.apple.madrid.plist” contains the “CloudKitSyncingEnabled” key and has a value set to “False,” indicating that text messages were not configured to synchronize with iCloud using the “Messages in iCloud” feature. When the iPhone 11 (FirstNet) was set up, the configurations and data were transferred from the iPhone 8 Plus (FirstNet) through the “Quick Start” feature. The setting controlling “Messages in iCloud” was included in that transfer, so the iPhone 11 (FirstNet) was initially set up with “Messages in iCloud” disabled.

In both the collections of the iPhone 11 (FirstNet) performed by Unit 42, the configuration file “com.apple.madrid.plist” contains the “CloudKitSyncingEnabled” key and has a value set to “True,” indicating that text messages were configured to synchronize with iCloud using the “Messages in iCloud” feature. Specifically, the change from “False” to “True” occurred on November 19, 2020, at 19:38:33 when “Messages in iCloud” was enabled based on the value of the “CloudKitInitialStartDate” key in the same configuration file.

This means that on November 19, 2020, before the iPhone 11 (FirstNet) was collected by Unit 42, the “Messages in iCloud” feature was enabled.

Backup Settings

In the August 21, 2020, and October 15, 2020 collections of the iPhone 11 (FirstNet), the configuration file “com.apple.mobile.ldbackup.plist” contains the “CloudBackupEnabled” key that is set to “False,” indicating that the device was not configured to automatically backup to iCloud at the time these two collections were performed. In these two collections, the configuration file “com.apple.mobile.ldbackup.plist” does not contain the “LastCloudBackupDate” key, indicating that the iPhone 11 (FirstNet) had not backed up to iCloud on or prior to October 15, 2020.

On November 16, 2020, Unit 42 inspected and preserved the iCloud account associated with this device and determined no iCloud backups for the iPhone 11 (FirstNet) or any other device were present in the iCloud account.

In both of the collections performed by Unit 42, the configuration file “com.apple.mobile.ldbackup.plist” contains the “CloudBackupEnabled” key set to “True,” and the “LastCloudBackupDate” key has a value representing the date November 19, 2020, at 19:47:58. This backup, created on November 19, 2020, is the first iCloud backup created for the iPhone 11 (FirstNet). Unit 42 confirmed this by reviewing the “Snapshots” table of the “cloudkit_cache.db” database located in the “/private/var/root/Library/Caches/Backup” folder. This table only listed one entry, and the “SnapshotsIDidx” index records the “Snapshots_rowid” for this entry as “1” indicating it was the first entry in the “Snapshots” table. The “Snapshots” entry had a “created” column with a value that also represented the date November 19, 2020, at 19:47:58.

This means that the iPhone 11 (FirstNet) was initially not configured to back up to iCloud. However, on November 19, 2020, before the iPhone was collected by Unit 42, back up to iCloud was enabled.

The "LastiTunesBackupDate" key in the "com.apple.mobile.ldbackup.plist" file contained values representing the last date on which an iTunes backup was created. In the August 21, 2020, and October 15, 2020, collections of the iPhone 11 (FirstNet), the "LastiTunesBackupDate" key contained a value representing the date August 21, 2020, at 19:29:09, the date of the iTunes backup of the iPhone 11 (FirstNet) identified on Ms. Chen's computer. In the collections performed by Unit 42, the value was October 15, 2020, at 20:23:02, which is the date of the collection created by the "Information Security Engineer" with the City.

Text/Chat Message Analysis

The August 21, 2020, backup contained active text messages dated from June 25, 2020, to August 21, 2020. The fact that, as of August 2020, the earliest text messages are dated June 25, 2020, is useful in determining which of the Message History settings led to the deletion of the Missing Durkan Text Messages. Had the "1 Year" setting been enabled, this backup should have contained active text messages dated at least one year prior, which would be August 2019. The fact that active messages only date back to June 25, 2020, is consistent with the "30 Days" option having been selected at one point but later changed back to keep messages "Forever," between July 22, 2020 PDT and July 26, 2020 PDT. The "chat" table located in the "sms.db" contained 325 active entries, of which 240 "chat" table entries had no associated messages in the "message" table. The backup of this phone having nearly 74 percent of entries in the "chat" table no longer associated with any messages is consistent with the Message History settings having been configured to retain either 30 days or one year of messages at some point in time. However, the dates of the messages still active in the "sms.db" are inconsistent with selection of the "1 Year" setting. Based on this information, Unit 42 infers that the "30 Day" setting was configured sometime on or after July 4, 2020 PDT, and before it was configured back to "Forever" between July 22, 2020 PDT and July 26, 2020 PDT.

Mayor Durkan Additional Analysis and Findings

Analysis of Data Sources Did Not Find the Missing Durkan Text Messages

Unit 42 analyzed the available data from all the sources collected in this matter related to Mayor Durkan's mobile devices, including iPhone data, iPhone backups, and iCloud data. None of these data sources filled in the Missing Durkan Text Messages between October 30, 2019, and June 25, 2020.

Timing of Retention Settings Changes

iPhones do not track, log, or otherwise record the timing when changes are made to the Message History setting "Keep Messages." The available data is consistent with the "30 Days" option having been set sometime on or after July 4, 2020 PDT, when the Disable & Delete messages function was used on the iPhone 8 Plus (FirstNet) and before the "Keep Messages" setting was changed back to keep messages "Forever" between July 22, 2020 PDT and July 26, 2020 PDT. The specific date in this time frame on which the "30 Days" option was set is not known and cannot be determined from the available data sources.

The window of time in which the "Keep Messages" setting would have been changed back to keep messages "Forever" can be inferred from the available data. This change could not have taken place later than 30 days after the oldest active text message (or more specifically, the time when that message would have been deleted had the "30 Days" setting remained active), otherwise that text message would have been automatically deleted by the "30 Days" setting. The oldest active text message is dated June 25, 2020, at 17:38:48 UTC. Thirty days later is July 25, 2020, at 17:38:48 UTC. After the initial deletion that occurs when setting the "Keep Messages" setting to "30 Days," automatic deletions by the Message History settings occur nightly at 03:00:00 local time. Therefore the "Keep Messages" setting must have been changed back to keep messages "Forever" prior to the next scheduled deletion event after July 25, 2020, at 17:38:48 UTC, which would be July 26, 2020, at 10:00:00 UTC (July 26, 2020, at 03:00:00 PDT). Furthermore, there is an entry in the "chat" table that has no associated messages, which is consistent with a chat that has had its associated messages deleted by the "Keep Messages" for "30 Days" option. The "chat" table indicates that the most recent message associated with this chat was dated June 23, 2020, at 06:11:47 UTC, from which Unit 42 infers that the "Keep Messages" setting was changed back to keep

messages “Forever” later than thirty days after this date, i.e., sometime after July 22, 2020, at 23:11:47 PDT (July 23, 2020, at 06:11:47 UTC).

Thus, while the precise date and time when the “Keep Messages” setting was changed from “30 Days” to “Forever” is not known, it can be deduced that the change occurred in the nearly 76-hour window (just over three days) between July 22, 2020, at 23:11:47 PDT and July 26, 2020, at 03:00:00 PDT. Throughout this report, references to the Message History being changed back to “Forever” “between July 22, 2020 PDT and July 26, 2020 PDT” and references to the “30 Day” setting changing after “July 4, 2020 PDT and before the configuration change between July 22, 2020 PDT and July 26, 2020 PDT” more precisely relate to the time range of July 22, 2020, at 23:11:47 PDT to July 26, 2020, at 03:00:00 PDT which listed in UTC would be July 23, 2020, at 06:11:47 UTC to July 26, 2020, at 10:00:00 UTC.

Accounting for Changes to iPhone Message History

Unit 42 was able to infer the actions that would have caused each change to the “KeepMessagesVersionID” based on analysis of the data sources from Mayor Durkan’s iPhone 8 Plus (Verizon) and iPhone 11 (FirstNet) and testing performed by Unit 42 on test devices to understand how functions related to “Messages in iCloud” affect text message retention. In the configuration file, “com.apple.MobileSMS.plist,” the keys “KeepMessageForDays” and “KeepMessagesVersionID” exist once the text message retention setting has been updated, either to “Forever” (the default value) or to “30 Days” or “1 Year.” When the text message retention setting is first updated, the “KeepMessagesVersionID” key will be created and its value set to “1.” That value is incremented by “1” with each successive update to the text message retention setting. The “KeepMessageForDays” key will have a value of “0,” “30,” or “365” to reflect the number of days corresponding to the text message retention setting. Other than manually updating the text message retention setting, Unit 42 also determined in its testing that enabling “Messages in iCloud” or selecting “Disable & Delete” for “Messages” within the “iCloud Storage” menu also updates the text message retention setting to “Forever,” (even if that was already the current setting) and also increments the value of “KeepMessagesVersionID.”

On the iPhone 8 Plus (Verizon), the “KeepMessageForDays” and “KeepMessagesVersionID” keys did not exist at the time of the August 29, 2019, iTunes backup. The absence of these keys means that the text Message History setting had never been updated as of August 29, 2019. When Unit 42 collected the iPhone 8 Plus (Verizon) on July 2, 2021, the “KeepMessageForDays” and “KeepMessagesVersionID” keys had values of “0” and “1,” respectively. This indicates that, prior to the phone being decommissioned on October 30, 2019, the text message retention setting was updated. Unit 42 found that “Messages in iCloud” was enabled on October 30, 2019. Enabling “Messages in iCloud” results in the Message History setting being updated to “Forever,” even if that is already the configured setting, thereby updating the “KeepMessageForDays” value and incrementing the “KeepMessagesVersionID” value.

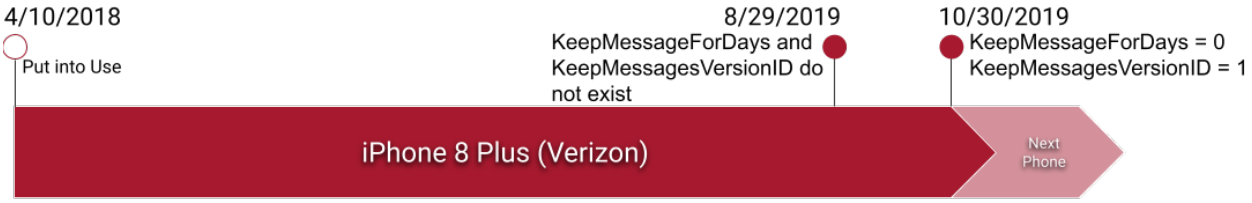


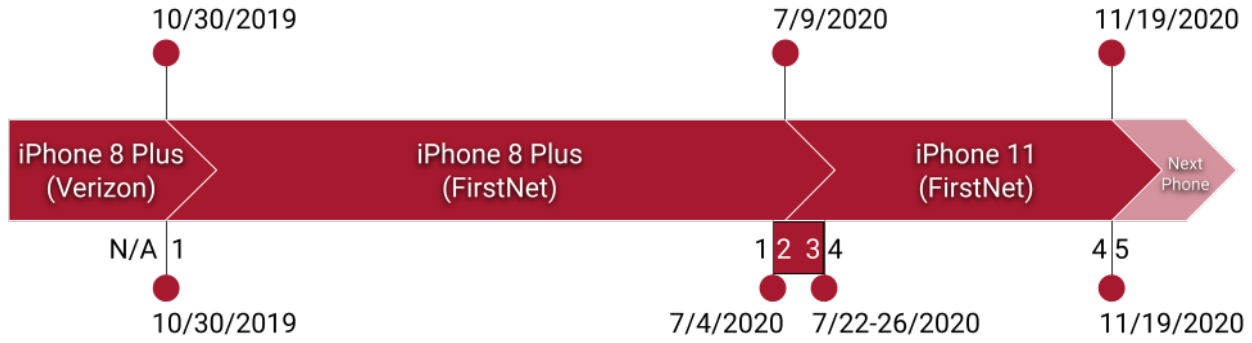
Figure 21 - A figure representing the presence and values of the “KeepMessageForDays” and “KeepMessagesVersionID” keys for the iPhone 8 Plus (Verizon)

In the August 21, 2020, iTunes backup of the iPhone 11 (FirstNet), the “KeepMessageForDays” and “KeepMessagesVersionID” keys had values of “0” and “4,” respectively. This indicates that the Message History setting had been updated three times between October 30, 2019, the decommission date of the iPhone 8 Plus (Verizon) on which “KeepMessagesVersionID” already had a value of “1,” and August 21, 2020.

When the iPhone 11 (FirstNet) was preserved by an "Information Security Engineer" with the City on October 15, 2020, the "KeepMessageForDays" and "KeepMessagesVersionID" keys had the same values of "0" and "4," respectively, as they did in the August 21, 2020, data source. When Unit 42 preserved the iPhone 11 (FirstNet) on November 19, 2020, the "KeepMessageForDays" and "KeepMessagesVersionID" had values of "0" and "5," indicating that there had been one additional update to the Message History setting between October 15, 2020, and November 19, 2020. Unit 42 found that "Messages in iCloud" was enabled on November 19, 2020, which would have resulted in the Message History setting being updated to "Forever," even if that was already the configured setting, thereby updating the "KeepMessageForDays" and "KeepMessagesVersionID" values.

Figure 22 - A figure representing the presence and values of the "KeepMessageForDays" and "KeepMessagesVersionID" keys for the iPhone 11 (FirstNet)

The following figure and table depict the inferences of Unit 42 concerning when the "KeepMessagesVersionID" key values were incremented based on analysis of configuration changes on Mayor Durkan's iPhones and the message gap between October 30, 2019, and June 25, 2020. The "KeepMessagesVersionID" key did not exist until October 30, 2019, at 19:40:35, when "Messages in iCloud" was enabled on the iPhone 8 Plus (Verizon), thereby creating the key and setting its value to "1." Based on Unit 42's analysis, on July 4, 2020, at 17:19:44 PDT, the "Messages" "Disable & Delete" function was used on the iPhone 8 Plus (FirstNet) which Unit 42 infers set the Message History setting to "Forever," even if that was the current setting, and incremented the "KeepMessagesVersionID" key from "1" to "2." After July 4, 2020, at 17:19:44 PDT and before the next configuration change between July 22, 2020 PDT and July 26, 2020 PDT, the Message History was set to "30 Days." This setting change increments the "KeepMessagesVersionID" key. Unit 42 infers that "KeepMessagesVersionID" incremented from "2" to "3" between July 4, 2020 PDT and the next configuration change between July 22, 2020 PDT and July 26, 2020 PDT, as depicted in the red box between these dates in the figure below. Unit 42 infers that the Message History was set to "Forever" between July 22, 2020 PDT and July 26, 2020 PDT which incremented "KeepMessagesVersionID" from "3" to "4." Lastly, on November 19, 2020, at 19:38:33, "Messages in iCloud" was enabled on the iPhone 11 (FirstNet) which incremented "KeepMessagesVersionID" from "4" to "5."



Date	Device	Action	KeepMessagesVersionID
10/30/2019	iPhone 8 Plus (Verizon)	"Messages in iCloud" Enabled	N/A → 1
07/04/2020	iPhone 8 Plus (FirstNet)	"Messages" "Disable & Delete"	1 → 2

Date	Device	Action	KeepMessagesVersionID
07/04/2020 to 07/22-26/2020	iPhone 8 Plus (FirstNet) / iPhone 11 (FirstNet)	Message History set to “30 Days”	2 → 3
07/22-26/2020	iPhone 11 (FirstNet)	Message History set to “Forever”	3 → 4
11/19/2020	iPhone 11 (FirstNet)	“Messages in iCloud” Enabled	4 → 5

Figure 23 - KeepMessagesVersionID Changes

Analysis of the text message database led Unit 42 to infer that the Message History setting had been changed to “30 Days” between July 4, 2020 PDT, after the “Disable & Delete” function had been used, and when the Message History setting had been changed to “Forever” between July 22, 2020 PDT and July 26, 2020 PDT. The precise date when the Message History setting changed to “30 Days” is unknown, so it has not been determined if that change occurred on the iPhone 8 Plus (FirstNet) or the iPhone 11 (FirstNet). On whichever device this change to the Message History occurred, the “KeepMessageForDays” key would have been set to “30,” which indicates that messages will be kept for 30 days, and the “KeepMessagesVersionID” key would have incremented from a value of “2” to “3.”

Inspection and Collection of iCloud Account

The first data source that Unit 42 collected in this matter was Mayor Durkan’s iCloud account, which was connected to all three of Mayor Durkan’s iPhones used from 2018 to the time Unit 42 was engaged, in November 2020. This iCloud account was examined, and data was collected on November 16, 2020, using forensic software from Magnet Forensics Inc. and Elcomsoft Ltd.

Data from Mayor Durkan’s iCloud account was collected first using the Magnet AXIOM Cloud forensic software. The software authenticated to the account and downloaded all available data. The AXIOM Cloud software downloaded data which showed that iCloud Drive contained no files. However, iCloud Photos did contain 230 images, which were all downloaded and preserved. No other data was available from Mayor Durkan’s iCloud account using the AXIOM Cloud software.

Next, additional collections of Mayor Durkan’s iCloud account were performed using Elcomsoft software to help ensure a thorough collection of available data. Using Elcomsoft, the iCloud account was examined for three types of data: backups, synchronized data, and files. Examination of the available backups shows that this iCloud account was not storing any backups of iPhones or other devices. Apple states that they only retain iCloud backups for 180 days after a device stops backing up to iCloud.[23] Finding no backups of any phones used within 180 days of examining the iCloud account would be consistent with those devices not being configured to save backups to iCloud. Any iPhones that went out of use more than 180 days before the examination of the iCloud account may or may not have been configured to backup to iCloud as any backups would have been automatically deleted by Apple after 180 days of inactivity.

Unit 42 sought to preserve synchronized data stored in the iCloud account. Synchronized data includes a number of types of data that are kept the same between an iPhone and an iCloud account, and are stored separately from any backups. Accessing some of the synchronized data, including any synchronized text messages, requires additional authentication steps to be performed. The additional authentication requires the input of a passcode from a trusted iPhone or other Apple device that is also synchronizing its “Keychain.” In November 2020, multiple attempts were made to access and download the synchronized data including the data requiring additional authentication, but iCloud would not accept the supplied passcode for additional authentication as valid. Any synchronized data that did not require additional authentication was

[23] For more information, see https://support.apple.com/guide/icloud/back-up-your-ios-and-ipados-device-mmab848634c8/icloud and https://www.apple.com/legal/internet-services/icloud/en/terms.html.

collected, but after multiple failed attempts to supply a correct passcode, Unit 42 halted the additional authentication attempts in order to prevent the iCloud account from locking and preventing access to any additional data that might be collected. In September 2021, after confirming that the iPhone in use by Mayor Durkan at that time was configured to synchronize its "Keychain," Unit 42 reattempted the preservation of any synchronized text messages using software from Elcomsoft. The account data and text messages were successfully preserved from Mayor Durkan's iCloud account at that time. Examination of the synchronized text messages preserved from iCloud showed that they included messages from June 25, 2020 through the date of the collection, September 9, 2021.

Finally, Unit 42 inspected and collected any files stored in the iCloud account. iCloud Drive contained no standard user files, but any available files were collected and preserved.

Pinnacle System

Unit 42 discussed the Pinnacle system with City IT resources and analyzed the Pinnacle Data Source provided by the City. Pinnacle is a custom-built application that the City uses to gather billing information from cellular phone providers in a centralized database. Unit 42 analyzed the Pinnacle Data Source and confirmed it to include data from January 2020 through the end of August 2020 for Mayor Durkan's mobile phone number. Analysis also confirmed that the Pinnacle Data Source included metadata for SMS text messages, but not Apple proprietary iMessage text messages. The Pinnacle Data Source provided no information on which we relied in completing our analysis of the goals described in this report (section titled Purpose of Our Engagement) other than confirming that Mayor Durkan sent and received messages during the time period from January 2020 through the end of August 2020.

Chief Best's iPhone XS Max Analysis and Findings

iPhone Setup Information

In the advanced logical collection representing Chief Best's iPhone XS Max, and its configuration as of September 2, 2020, the configuration file "com.apple.MobileBackup.plist" contains the "RestoreDate" key and has a value that represents October 1, 2019, at 18:27:45, as seen in the following figure. Additionally, the "WasCloudRestore" key in the same configuration file has a value of "False," indicating that the Best iPhone XS Max was not set up by a restoration from an iCloud backup, but rather a restoration from another phone, specifically the Best iPhone 8 Plus.

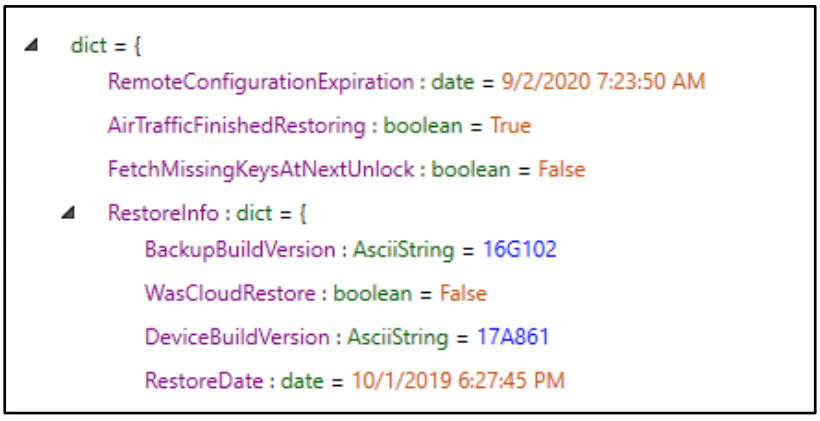


Figure 24 - A screenshot of a limited preview of the "com.apple.MobileBackup.plist" file from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Also in the advanced logical collection, the configuration file "com.apple.purplebuddy.plist," contains the "GuessedCountry" key which has a subkey named "at," that has a value that represents December 1, 2019,

at 10:12:19, the date the “Select Your Country or Region” option was selected. The “SetupLastExit” key has a value that represents December 1, 2019, at 14:21:37, the date that the setup application was last completed. This sequence of events is consistent with the phone having been restored from the previous phone on October 1, 2019, yet the setup process was last completed on December 1, 2019. This pattern is consistent with a phone that was set up initially through restoration from a previous phone, but then completed the setup routine again, as is encountered for example, after installing a major update to the Apple iOS operating system. The following figure shows an excerpt of the “com.apple.purplebuddy.plist” configuration file.

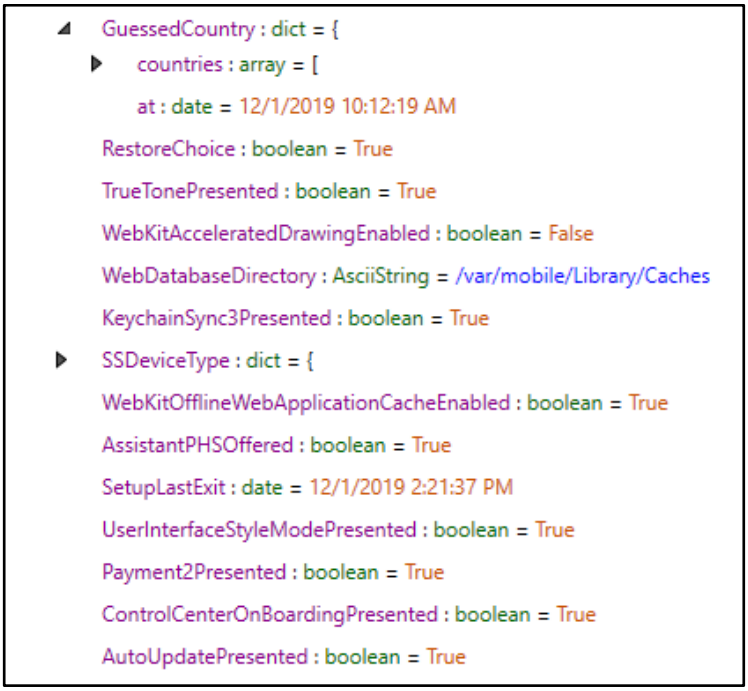


Figure 25 - A screenshot of a limited preview of the “com.apple.purplebuddy.plist” file from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Text Message Retention Settings

The configuration file “com.apple.MobileSMS.plist,” as seen in the following figure, contains the “KeepMessageForDays” key, which has a value of “30,” indicating any text messages older than 30 days stored locally on this iPhone would be automatically deleted by the iPhone on a nightly, rolling basis.

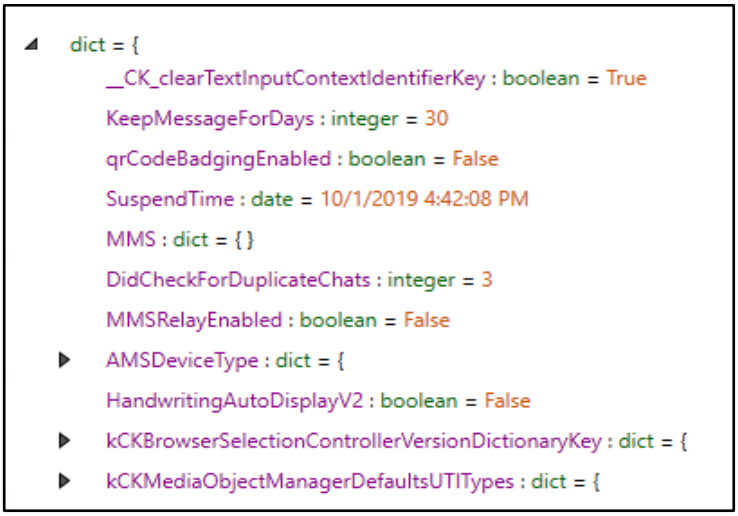


Figure 26 - A screenshot of a limited preview of the "com.apple.MobileSMS.plist" file from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Synchronizing Messages to iCloud Settings

The configuration file "com.apple.madrid.plist" contains the "CloudKitSyncingEnabled" key and has a value set to "False," indicating that text messages were not configured to synchronize with iCloud using the "Messages in iCloud" feature. The same configuration file also has keys, such as "CloudKitSyncDate," "CloudKitInitialStartDate," and "LastChatSyncTime," that have values representing dates between April 2019 and May 2019. This indicates that at no time would the Best iPhone XS Max have been configured to synchronize with iCloud using the "Messages in iCloud" feature, as these dates predate the initial set up of this phone. All of these keys, as well as others, can be seen in the following figure.

Figure 27 - A screenshot of a limited preview of the "com.apple.madrid.plist" file from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Backup Settings

The configuration file "com.apple.mobile.ldbackup.plist" contains the "CloudBackupEnabled" key with a value of "True," indicating that the device was configured to automatically backup to iCloud at the time this phone went out of use. However, the same configuration file contains the "LastCloudBackupDate" key with a value that represents October 1, 2019, at 18:23:38. This date and time is a few minutes earlier than the setup of this iPhone. A "LastCloudBackupDate" date predating the setup of the phone is consistent with this date having been carried over from the previous phone when data was restored onto the Best iPhone XS Max. This means that the Best iPhone XS Max was never backed up to iCloud, even though it was configured to do so, possibly due to a lack of available storage space in the iCloud account. These keys can be seen in the following figure.

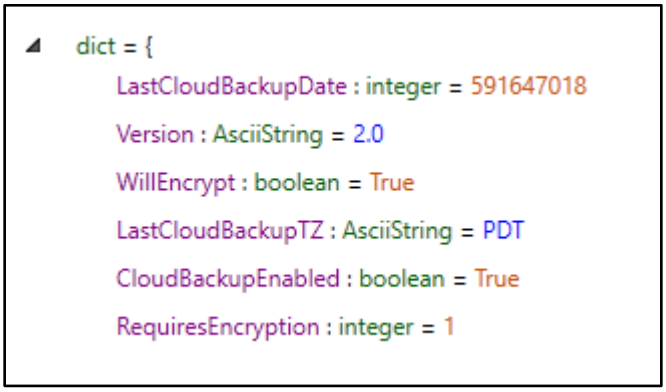


Figure 28 - A screenshot of a limited preview of the "com.apple.mobile.ldbackup.plist" file from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.47.0.49) (Times displayed are in UTC.)

Text/Chat Message Analysis

In the advanced logical collection, the "sms.db" file contains 64 entries in the "message" table. Of those entries, only 15 have an "item_type" of "0," which signifies standard text messages. The remaining 49 entries in the "message" table have an "item_type" of "1," which are internal database entries created when group chats occur. These 49 entries do not have any message text and are not visible to a user. While there may be 64 total entries in the "message" table, the total number of text messages is 15. These 15 messages are all dated September 2, 2020, from 8:26:30 PDT to 12:27:21 PDT. The following figure shows a portion of the "message" table in the "sms.db" database where these 15 and 49 entries, 64 in total, can be seen.

ROWID	guid	text	date	item_type	service	handle_id	other_handle
25985	2C9816BB-067B-4979-8D40-16DFD086445A		8/3/2020 9:46:55 PM	1	iMessage	3728	3728
25986	A3FBEB57-1406-45BB-9438-31455D80A47D		8/3/2020 9:46:55 PM	1	iMessage	3728	3784
26026	69F4E8F2-3480-4D5A-A110-78205C79B6EA		8/4/2020 3:21:03 PM	1	iMessage	64	1423
26027	3B70551B-8465-4328-8018-206F4AC5FA7E		8/4/2020 3:21:03 PM	1	iMessage	64	65
26028	5D6CB671-5800-475A-BFA5-42F878B002EE		8/4/2020 3:21:03 PM	1	iMessage	64	64
26029	A570F20C-3B52-4A0F-8BF6-1A3620896F55		8/4/2020 3:21:03 PM	1	iMessage	64	66
26339	9FA8C844-5D6F-4092-AAB2-3919F48DBF3F		8/10/2020 3:41:30 PM	1	iMessage	64	65
26340	0EFF660A-88C6-4A22-BB0A-191DFEAD26B6		8/10/2020 3:41:30 PM	1	iMessage	64	64
26341	73C09E52-74B3-4BA0-B640-F1D02EB2E469		8/10/2020 3:41:30 PM	1	iMessage	64	66
26381	90B94A20-2C75-4AC5-BD1E-103CCA68A06C		8/11/2020 4:24:21 AM	1	iMessage	3441	34
26382	4ECE2246-BA0C-4239-9E1A-00C31914BB73		8/11/2020 4:24:21 AM	1	iMessage	3441	3441
26494	0FBD56A7-953F-4C15-87FE-6A7AC75B3DEB		8/11/2020 3:38:10 PM	1	iMessage	3410	34
26495	FB020359-B2A5-4337-84BE-79B4189E75ED		8/11/2020 3:38:10 PM	1	iMessage	3410	3410
26522	6814ADD5-9242-4BB6-BBC5-2C42A9671DBF		8/11/2020 5:24:12 PM	1	iMessage	2562	919
26523	3FBE20DD-DB1B-4543-AC68-6D0437822005		8/11/2020 5:24:12 PM	1	iMessage	2562	2562
26604	8D58F954-8879-4019-AB92-C776627FC884		8/12/2020 6:05:45 PM	1	iMessage	3926	3927
26605	80A87968-EC17-439C-8960-C3421885D573		8/12/2020 6:05:45 PM	1	iMessage	3926	3926
26680	D549B29B-96D9-4559-AE00-51C6DA41EFCD		8/13/2020 4:56:03 AM	1	iMessage	919	1423
26681	B1B7BFA8-802E-42FE-8B18-FD3104AD9984		8/13/2020 4:56:03 AM	1	iMessage	919	919
26682	7724C1C3-8716-476E-B033-9A919D8DAEF4		8/13/2020 4:56:03 AM	1	iMessage	919	3936
26683	28432067-FFC7-49AA-824F-284F5AB644A0		8/13/2020 4:56:03 AM	1	iMessage	919	66
26708	19E753AA-A9EB-4357-890A-0B0385279A75		8/13/2020 9:56:43 PM	1	iMessage	919	1423
26709	C6C43CDA-07A5-4C7E-87DB-2DEEED235D73		8/13/2020 9:56:43 PM	1	iMessage	919	65
26710	3DE3994D-67B8-44AC-B9E0-FC062F072610		8/13/2020 9:56:43 PM	1	iMessage	919	64
26711	E38C426A-FF93-4D96-9BBB-80C5872D6EE7		8/13/2020 9:56:43 PM	1	iMessage	919	919
26712	25D69682-F2F8-47E0-B7BE-8A0A5B6938DD		8/13/2020 9:56:43 PM	1	iMessage	919	66
26779	8DD62AA9-932C-447C-814A-49998CB22AEE		8/15/2020 10:30:58 PM	1	iMessage	66	2683
26780	A51A27FD-D382-44CD-AD95-33F3CABFC20D		8/15/2020 10:30:58 PM	1	iMessage	66	65
26781	36F7EA75-3308-4714-94D0-DFA69D14AA43		8/15/2020 10:30:58 PM	1	iMessage	66	66
26782	08221C01-7525-407C-B61D-2C7023DC2FF0		8/15/2020 10:30:58 PM	1	iMessage	66	2501
26783	CE355ED8-335F-4DF1-A3E2-144AC9B9FCE0		8/15/2020 10:30:58 PM	1	iMessage	66	919
26784	6C14D421-8B89-41C2-B5BA-564AFB2774B3		8/15/2020 10:30:58 PM	1	iMessage	66	623
26824	86F017C2-EE8D-4F2E-A150-36CC468DBFE6		8/16/2020 11:30:56 PM	1	iMessage	919	1423
26825	FFF20A9E-A9AE-411A-B153-11B616B068FE		8/16/2020 11:30:57 PM	1	iMessage	919	919
26826	E441FB09-5929-4927-A5F6-1AADDF86BE34		8/16/2020 11:30:57 PM	1	iMessage	919	3936
26827	9D5588E2-14D3-415F-BAAF-92137BAC52CB		8/16/2020 11:30:57 PM	1	iMessage	919	66
26840	5DAD49C4-886E-41EB-BBDC-CFC7B97FC812		8/17/2020 3:21:39 PM	1	iMessage	65	2683
26841	D09C2766-2654-43C9-B40E-A27B420DEDC5		8/17/2020 3:21:39 PM	1	iMessage	65	65
26842	AAD1C8A6-D66D-48D3-BDEF-9E3943C94B4F		8/17/2020 3:21:39 PM	1	iMessage	65	919
26843	EF815160-C144-47D8-95D7-F2E7DAEF9A36		8/17/2020 3:21:39 PM	1	iMessage	65	66
26945	3C576A12-B6EA-4179-A4D3-16D16C9900C7		8/21/2020 1:45:29 AM	1	iMessage	3973	3974
26946	5E5CED89-7002-4C4F-8C90-FB0BEFFD895F		8/21/2020 1:45:29 AM	1	iMessage	3973	3973
26956	8E5B89FD-5C08-4569-80B8-ED99B623D55D		8/21/2020 12:12:51 PM	1	iMessage	3410	1218
26957	6E51686A-B32E-435E-B29B-3F204CCB9EDA		8/21/2020 12:12:51 PM	1	iMessage	3410	3784
26958	55BB51C0-0A99-46FA-A55A-CDFB6875C6CE		8/21/2020 12:12:51 PM	1	iMessage	3410	3410
27027	82D234DE-C130-4077-A80B-E3D18C003FA5		8/26/2020 12:10:02 AM	1	iMessage	3441	34
27028	6BBB52AD-A5C8-4A39-8289-111BC99F3F13		8/26/2020 12:10:02 AM	1	iMessage	3441	3441
27031	1D26F4B9-0BF6-4A86-8BE3-512310C6D111		8/26/2020 12:16:29 AM	1	iMessage	3441	34
27032	BD92065A-C6CA-4176-B783-2CD075AA37C2		8/26/2020 12:16:29 AM	1	iMessage	3441	3441
27188	37484E1C-7A88-7537-A4F1-14288E6516BF	Shooting 9026 Seward PK Ave S(atlantic boat ramp 1 Person shot, suspect outstanding 3R 20...	9/2/2020 4:48:21 PM	0	SMS	4039	0
27189	6DC75226-AF2D-432D-8B7B-386EA948AD60	ASLT - IP/JO - PERSON SHOT OR SHOT AT 20:17:34 RAINIER AV S / S KENYON ST[NORTH OF...	9/2/2020 7:27:19 PM	0	SMS	4040	0
27190	4EEE563B-7C73-78A5-C748-E917DF7DA52D	Stabbing 200 Lake WA BV E 1 person stabbed suspect outstanding 3Q 206-889-2374 #6139	9/2/2020 7:27:19 PM	0	SMS	4039	0
27191	24CEC7DC-4198-418A-B137-14C145A6703B	The call type for call # 256171 has been changed from SHOTS1 to SHOOT1 Sent by: WD	9/2/2020 7:27:19 PM	0	SMS	4041	0
27192	ACE48E2F-7C91-81B3-31BF-B29BDE77ABB0	Shots Fired 3 Av & Yesler Wy Gunshots in area. Shell casings and blood drops found. Checkin...	9/2/2020 7:27:20 PM	0	SMS	4039	0
27193	C3BCCA53-E005-48AF-AF35-9E9AC1F91383	ASLT - IP/JO - PERSON SHOT OR SHOT AT 22:46:16 325 9 AV Dt: G Zne: G1 Gd: 4043 HMC A...	9/2/2020 7:27:20 PM	0	SMS	4042	0
27194	3AD06BA0-D409-435B-BEED-F379A57E1658	ASLT - IP/JO - PERSON SHOT OR SHOT AT 23:08:33 700 MINOR AV Dt: E Zne: E3 Gd: 6245 S...	9/2/2020 7:27:20 PM	0	SMS	4043	0
27195	85F8940A-E0B8-6A29-5890-585951527269	Follow Up to Shots Fired 3 Av & Yesler Wy 2 gunshot victims arrived at HMC & Swedish. Appe...	9/2/2020 7:27:20 PM	0	SMS	4039	0
27196	F732BE6D-DBE7-4090-AF2E-90A71160F427	ASLT - IP/JO - PERSON SHOT OR SHOT AT 23:33:29 925 SENECA ST Dt: E Zne: E3 Gd: 3519 V...	9/2/2020 7:27:20 PM	0	SMS	4044	0
27197	C06AA69E-BFA7-3120-B079-D96710B92A3A	Happy last day, Chief. It's been an honor. I hope you get all the fun and joy and space in your r...	9/2/2020 7:27:20 PM	0	SMS	4045	0
27198	321AEE8C-8583-0717-1B53-6A67D9B6EFCF	Hi there Carmen, before your departure today I just want to touch base to thank you for your l...	9/2/2020 7:27:21 PM	0	SMS	4046	0
27199	EF3BD0D2-DF0E-0045-34A2-BCFC16771E44	I personally wanted to reach out to you with possible future opportunities where you can con...	9/2/2020 7:27:21 PM	0	SMS	4046	0
27200	ADB8C34D-79FB-4289-AF25-DB93CCAAD750	Congratulations on a well-deserved retirement and for handling these past three months with...	9/2/2020 3:26:30 PM	0	iMessage	4047	0
27201	62018F52-C4B5-4968-BDF9-89731A5A1A7D	Happy last day, Chief. It's been an honor. I hope you get all the fun and joy and space in your r...	9/2/2020 4:35:24 PM	0	iMessage	4048	0
27202	61C45768-3CA7-41FA-B9A2-96EBB63E45FB	ASLT - IP/JO - PERSON SHOT OR SHOT AT 19:40:14 9026 SEWARD PARK AV S Dt: S Zne: S2...	9/2/2020 4:48:19 PM	0	SMS	4049	0

Figure 29 - A screenshot of a limited preview of the "message" table in the "sms.db" database from the advanced logical collection of the Best iPhone XS Max as viewed in Cellebrite Physical Analyzer (v7.49.0.28) (Times displayed are in UTC.)

As previously discussed in this report, when the "30 Days" text message retention setting causes an iPhone to automatically delete messages older than the configured retention period, the corresponding entries in the "sms.db" "message" table are removed, but the related entries in the "chat" table are left in place. The "sms.db" file on the Best iPhone XS Max has a total of 28 entries in the "chat" table, 11 of which related to the 15 active text messages. The remaining 17 entries in the "chat" table are not associated with any entries in the "message" table. These 17 entries are consistent with messages related to these "chat" entries having been deleted by the "30 Days" setting. The maximum "ROWID" in the "chat" table was 5,133. This number indicates that there were a total of 5,133 entries created into the "chat" table from November 5, 2018 (when the Best iPhone 8 Plus was set up) to September 2, 2020 when the Best iPhone XS Max went out-of-use.

Had Chief Best been sending and receiving text messages with the "30 Days" retention setting configured and had she left those text messages to exist past 30 days, messages would have been deleted

automatically due to the retention setting and a large number of entries in the “chat” table that were not associated with any entries in the “message” table would have resulted. In contrast, the artifacts reviewed on the Best iPhone XS Max are consistent with periodic deletion over time rather than a bulk deletion. The very low number of entries in the “chat” table that do not relate to entries in the “message” table is consistent with Chief Best’s testimony in her deposition;[24] that she deleted text messages periodically.

Dated: February 11, 2022

Respectfully submitted,

Kevin T. Faulkner

[24] Chief Best 11/9/2021 Dep. Tr. at 212:13-213:2, 213:17-214:11, 214:21- 216:4-16, and 217:5-15.

Kevin Faulkner

PALO ALTO NETWORKS (Formerly Crypsis; Acquired in 2020)
Vice President, February 2019 to Present
New York, NY

Lead teams in digital forensic and cybersecurity incident response investigations in connection with internal investigations, data breach incidents, civil or criminal litigation, and regulatory matters.

STROZ FRIEDBERG
Managing Director, March 2017 to December 2018
Vice President, November 2015 to March 2017
Director, Digital Forensics, November 2014 to October 2015
New York, NY

Head of the New York digital forensics lab. Co-managed the firm's technical operations in areas of digital forensics, electronic discovery, and incident response. Supervised and performed digital forensic acquisitions and examinations on laptop and desktop computers, e-mail and file servers, handheld/mobile devices, backup tapes and network logs. Maintained an active case load of digital forensics engagements in internal investigations and civil, criminal, and regulatory matters as well as cybercrime engagements. Types of analysis included (but were not limited to) document authentication, the theft or misappropriation of intellectual property or other data, database analytics, loss of data under legal hold, computer hardware forensics and data recovery, and investigations into computer intrusions or hacking.

Significant casework included:

- Led a team of forensic examiners and incident responders in an investigation into a data breach where the records of a healthcare company were identified by a third party on the "Dark Web". Analysis consisted of determining the original system the attacker used to penetrate the network, determining that other systems were accessed, what data may have been exfiltrated, and confirming which systems actually contained sensitive PII and PHI data.
- Performed analysis of primary central database for large retailer in connection with the sale of assets. Database needed to have certain customer and sales information removed prior to being delivered to buyer, involving the searching and correlation of hundreds of millions of records.
- Led a team responding on short notice to a security incident for a large retailer involving sophisticated file-less malware running on several dozen company servers, workstations, and laptops. Performed memory analysis, captured and analyzed network traffic, and pieced together forensic artifacts to understand what the attacker was doing, what systems they accessed, and what data may have been taken.
- Led a team to inventory, collect, and acquire technology for two related companies in bankruptcy. Identified several hundred computers, hard drives, servers, virtual servers, and other technology and worked with restructuring team to prioritize and create an efficient process for collection and imaging. Helped team locate and extract useful data for ongoing financial analysis and investigation.
- Assisted financial institution with several thousand backup tapes to attempt to locate data required to respond to inquiries from the federal government. Many tapes were from systems no longer in use at the client, where both the technology and staff related to the tapes were no longer with the company. Analyzed written and digital tape information to narrow down and locate potentially relevant information.
- Examined embedded credit card skimmer in point-of-sale device for a hospitality company. Identified the components used as pieces from a commercial handheld skimmer. Created custom process to recover password protecting the stored card data. Successfully accessed stored card swipe data and provided actionable information to client.
- Analyzed one commercial hand-held credit card skimmer and one pin-pad overlay skimmer for a major retailer. Performed hardware analysis to determine the local storage capacity of skimmer devices and the methods available for retrieving stored data, both by the attacker and by our team. Removed memory chip in a "chip-off" procedure and successfully accessed stored card swipe information. Identified storage format of card swipe data to provide actionable data to client.
- Oversaw the analysis of voice recording systems at a large energy company to determine the extent and cause of calls being over-recorded, leading to potential issues with regulators.
- Led teams of forensic examiners in investigation and eDiscovery response for large industrial products distributor in response to FTC investigation. Coordinated collections from custodians located around the continental U.S. Managed custom processing specifications to locate and process information beyond the scope of standard eDiscovery projects. Consulted with counsel to help ensure compliance and create good will with FTC investigations team.

- Consulted with in-house computer security team at large software solutions and services company providing one of the largest credit application networks in North America. Led forensic investigation and malware analysis in a network intrusion where an attacker had gained access to a network device and deployed malware to be used for DDOS purposes.
- Investigated authenticity of email messages purportedly sent in a business deal with China involving hundreds of billions of U.S. dollars. Was able to identify indicators consistent with email messages having been modified.
- Led team of forensic examiners in a data remediation matter where a high-level individual in the insurance industry went to a competitor after over a decade with his former employer. Established protocol for data identification and remediation to protect former employer's information and executed protocol on multiple personal devices.
- Acted as quality assurance on an important document forgery case by completing an independent analysis on the forensic images of computers that had been previously analyzed by another firm. Identified forensic indicators that led to the discovery of additional devices storing potentially relevant information and completed analysis of all devices still in existence.

MESIROW FINANCIAL CONSULTING
Senior Vice President, August 2012 to November 2014
New York, New York

Led the Technology Advisory Services (TAS) practice, a team of experts that focused on Computer Forensics, Electronic Discovery, Computer Security, and Data Analytics / Data Transformation. Helped clients in litigation, bankruptcy, or with internal security or investigative matters, understood and balanced the risks with cost saving options to get clients to a better resolution. Utilized years of technology and legal experience to help clients navigate the challenges that arose and found creative, intelligent solutions.

PROTIVITI
Director, Computer Forensics and eDiscovery, March 2006 to June 2012
New York, NY

Key component of the Computer Forensics, Electronic Discovery, and Records Management team. Continued work as an expert in the courts and expanded to include State, Federal, Chancery, and Bankruptcy courts. Prepared affidavits, declarations, and expert reports, and offered testimony in deposition, at hearings, and as an expert witness at trial in courts across the country. Functioned as a third-party neutral expert and handled sensitive data to help resolve issues of spoliation.

Significant matters included:

- Significantly expanded Computer Security incident response and investigation capabilities and achieved Qualified Security Assessor (QSA) certification from the PCI Security Standards Council.
- Led the Computer Forensics and Electronic Discovery team in Protiviti's New York office and expanded the group's capabilities in Chicago, Orlando, Dallas, Los Angeles, London, Paris, Frankfurt, Beijing, Hong Kong, New Delhi, Hyderabad, and Tokyo.
- Offered data collection, eDiscovery processing, and forensic / security investigation services utilizing a mix of local and remote resources to provide clients with the best combination of expertise and cost savings, resulting in exceptional value.
- Led evidence preservation effort in April 2011 for the Sony PlayStation Network attack by the hacker group Anonymous. Was first responder on-site. Technically challenging preservation required adherence to both legal and PCI (Payment Card Industry) standards due to possibility of credit card breach. Successfully navigated technical and legal / regulatory challenges and developed method for evidence preservation used going forward.
- Led forensic analysis and investigation in 2011 into Confidential Foreign Government's computer systems after attack by an unknown, outside attacker or group using advanced and custom malware in an APT (Advanced Persistent Threat). Identified method of attack, method of data transmission, and numerous additional affected computer systems not originally thought to be included in the attack. Helped client identify some of the stolen information and developed a remediation plan to address ongoing security concerns.
- Inspected computer systems at Raritan's payroll vendor ADS in 2011 in relation to Gannett Satellite v. Borough of Raritan, Docket No. L- 001798-09 (N.J. Super. Ct. Law Div. Oct. 06, 2009). Filed expert report and testified as expert witness for April 2012.

PG LEWIS & ASSOCIATES
Forensic Examiner and Case Manager, December 2003 to March 2006
Whitehouse Station, NJ

Performed forensic acquisitions or collections and successfully extracted and captured data while following forensic protocols. Assisted in investigations and forensic examinations. Became the highest level technical resource on the team, having gained significant skill in using EnCase from Guidance Software, FTK from AccessData, and other forensic tools. Led forensic investigation and electronic discovery projects, consulted with clients and their legal counsel, managed teams of people on the acquisition and examination, and provided the final level of review before materials went to the client. Worked as an expert in state and federal courts. Deposed, authored affidavits, declarations, and expert reports on multiple matters as well as attended hearings and trial.

FIDELIA TECHNOLOGY
Support Engineer, February 2003 to December 2003
Princeton, NJ

Aided with all aspects of monitoring product, from consulting with the programming team and leadership on product development, to assisting in the sales cycle as a technical expert, to supporting existing clients and performing implementations. Maintained the company's IT infrastructure in their Princeton, NJ headquarters.

MEASURABLE SOLUTIONS
Systems and Network Management Consultant, July 2000 to August 2002
Rockaway, NY

Consulted with clients to understand their technology infrastructure and identify the components that were business critical. Helped clients choose from amongst the best of breed monitoring products and helped them implement and integrate the products together into an overall monitoring solution.

MAINTECH / VOLT INFORMATION SCIENCES
Systems and Network Management Consultant, July 2000 to July 2000
Warren, NJ

Designed, implemented, supported, and repaired networks, servers, and PCs. Continued to build the depth of technical skills as well as gained broad experience with the technologies involved in large datacenters and vast wide area networks.

MC^2
Network Services Engineer, July 1998 to April 1999
Warren, NJ

Worked on computer systems of all types and sizes from PCs and small networks to large datacenters. Designed, implemented, supported, and repaired networks, servers, and PCs on the east coast.

CERTIFICATIONS AND AFFILIATIONS

2004 to 2023: EnCase Certified Examiner (EnCE), OpenText (formerly Guidance Software)
2005 to 2022: Certified Computer Examiner (CCE), International Society of Forensic Computer Examiners
2014 to 2024 : GIAC Certified Forensic Examiner (GCFE), Global Information Assurance Certification
2011 to 2012: PCI Qualified Security Assessor (QSA), Payment Card Industry (PCI) Security Standards Council
2006 – Present: CompTIA Linux+, CompTIA
1999 to Present: Microsoft Certified Professional including Windows XP, NT4 Server, Windows 95, Microsoft
Member, Sedona Conference WG1 & WG6 & WG11
Member, Association of Certified Fraud Examiners (ACFE)
Member, International Society of Forensic Computer Examiners (ISFCE)

TRAINING

Stroz Friedberg Internal Cyber Training Program
Participate in regular in-house training presentations on current digital forensics, cybercrime response, computer security, desktop, and network forensic tools in conjunction with relevant legal and industry matters

PUBLICATIONS

July 2013: *Changing Risks In eDiscovery*, eDiscovery Compendium issue, eForensics Magazine

TESTIMONY

November 2021: Provided expert response to a witness statement regarding technology issues in extracting data from email archives in *Biomet c.s. v. Heraeus Medical GmbH*, District Court of Rotterdam, The Netherlands, Case No. C/10/581437 / HA ZA 19/0817

August 2021 to October 2021: Submitted two expert reports and testified in deposition related to allegations of theft of trade secrets, in the matter of, *Comet Technologies USA Inc., et al. v. XP Power LLC.*, The United States District Court for the Northern District of California, Case No. 5:20-cv-06408-NC

May 2021 to July 2021: Provided rebuttal expert report, declaration, and testified in deposition regarding allegations of theft of trade secrets during the M&A due diligence process in *TransPerfect Global, Inc. v. Lionbridge Technologies, Inc., et al.*, The United States District Court for the Southern District of New York, Case No. 1:19-cv-03283-DLC

April 2021 to June 2021: Submitted two declarations and testified at two evidentiary hearings regarding how Apple devices lock to iCloud accounts, how one iPhone became factory reset, and deletion patterns and message retention settings for iPhones in a False Claims Act case, *United States ex rel. Purcell v. Gilead Sciences, Inc.*, The United States District Court for the Eastern District of Pennsylvania, Case No. 2:17-cv-3523-MAK

March 2021 to April 2021: Provided rebuttal expert report and deposition testimony in a case involving allegations of trade secret misappropriation in *Zimmer Biomet v. Heraeus Medical, LLC, et al.*, Kosciusko County Superior Court 4, State of Indiana, Case No. 43D04-1802-PL-000021

January 2021: Affidavit covering mobile forensic issues regarding text messaging data produced by opposing side in *Mariah Carey v. Lianna Shakhnazarian (a/k/a Lianna Azarian),* Supreme Court of The State of New York, County of New York, Index No. 0650290/2019

August 2020 to October 2020: Provided rebuttal expert report, testified in deposition as well as at the trial-type official administrative hearing in a case involving allegations of trade secret misappropriation in the matter of, *Certain Bone Cement and Bone Cement Accessories*, United States International Trade Commission, Washington D.C., Investigation No. 337-TA-1175

July 2020: Provided declaration regarding efforts to access encrypted data from mobile devices in *Lianna Shakhnazaryan v. Mirage Entertainment, Inc., Mariah Carey, et al.,* Superior Court of The State of California, County of Los Angeles, Central District, Case No. 19STCV01308 and 19STCV02516

May 2020: Provided expert analysis and a declaration for a third party subpoenaed for records in litigation in *Chevron Corporation v. Steven Donziger, et al.*, The United States District Court for the Southern District of New York, Case No. 1:11-cv-00691-LAK-RWL

September 2019: Submitted an affidavit in support of an application for a temporary restraining order and preliminary injunction in a matter where a former employee was accessing sensitive data from their former company and publishing it publicly, Supreme Court of The State of New York, County of New York, No case number, pre-litigation

August 2019: Provided written testimony in the form of a rebuttal expert report in a matter involving alleged trade secret misappropriation in *SS&C Technologies, Inc. v. Clearwater Analytics, LLC,* Connecticut Superior Court, Hartford, Complex Litigation, Case No. X07-HHD-CV-16-6070536-S

August 2018 to October 2018: Provided written testimony in the form of a rebuttal expert report, declaration, and testified in deposition regarding forensic analysis and expert opinions of computer systems used by one engineering team in *Synopsys, Inc. v. Ubiquiti Networks, Inc. et al.,* The United States District Court for the Northern District of California, Case No. 3:17-cv-00561-WHO

April 2017 to January 2018: Provided written testimony in the form of several declarations, multiple expert reports, and testified in three depositions on the collection and search processes used to preserve and search digital evidence regarding allegations of theft of trade secrets in *Waymo LLC v. Uber Technologies, Inc. et al.,* The United States District Court for the Northern District of California, San Francisco Division, Case No. 3:17-cv-00939-WHA

August 2017: Submitted declaration about wiping of devices by a departing employee in *International Business Machines Corporation v. Smith,* The United States District Court for the Southern District of New York, Case No. 7:17-cv-05808-CS-PED

August 2016 to October 2016: Provided written testimony in the form of a report and declaration regarding the wiping of data and rebuttal of another expert in *Schreiber v. Friedman et al.*, The United States District Court for the Eastern District of New York, Case No. 1:15-cv-06861-CBA-JO

February 2016: Provided a report as a court appointed expert in digital forensics centered around the analysis of artifacts on a mobile phone related to the creation and deletion of video and picture files in *Pagan v. The City of New York et al.,* The United States District Court for the Eastern District of New York, Case No. 1:15-cv-05825-LDH-RLM

May 2015: Testified in deposition about large-scale database analysis for cellular phone providers in *RS Legacy Corporation fka RadioShack Corporation*, The United States Bankruptcy Court, District of Delaware, Case No. 1:15-bk-10197-BLS

January 2015: Submitted declaration on behalf of a subpoenaed third party discussing analysis of their systems to identify files potentially taken from Plaintiff in a thief of intellectual property case, *Applied Materials, Inc. v. Burks*, The United States District Court for the Northern District of New York, Case No. 1:14-cv-01346-GTS-CFH

November 2013: Testified at arbitration as a digital forensics expert regarding analysis of messages from mobile devices in *MLB Players Association v. Office of the Commissioner of Baseball*, The Major League Baseball Arbitration Panel, Grievance No. 2013-2 (Alexander Rodriguez)

June 2012: Submitted an affidavit relating to the plaintiff's spoliation of data after forensically examining the plaintiff's computer evidence in an alleged copyright infringement case, *Gordon v. DreamWorks Animation SKG, Inc., et al.,* The United States District Court for the District of Massachusetts, Case No. 1:11-cv-10255-JLT

December 2011 to April 2012: Submitted an expert report, declaration, and testified at trial as a digital forensics expert regarding computer systems, payroll process and data in *Gannett Satellite v. Borough of Raritan,* New Jersey Superior Court, Law Division, Case No. L-001798-09

February 2012: Functioned as a third-party neutral expert, helped to refine and execute a search protocol to provide needed data to the right parties without disclosing confidential information in a theft of intellectual property matter, *CBR Systems, Inc., v. Christopher Deigan,* New Jersey Superior Court, Chancery Division, Case No. BER-C-383-11

November 2011: Testified in deposition on the evidence preservation process for the Thornburg Mortgage Chapter 11 bankruptcy, *Joel Sher v. SAF Financial, Inc. et al.*, The United States District Court for the District of Maryland, Case No. 1:10-cv-01895-RDB

September 2009: Submitted expert report and testified in deposition and at trial as a third-party neutral digital forensics expert on the potential destruction of data, comparison of sets of data, and other digital forensic issues in *T R Investors LLC v. Arie Genger*, Court of Chancery of the State of Delaware, Civil Action No. 3994-VCS

May 2009 to July 2009: Provided written testimony in the form of multiple declarations on the process used and conclusions reached by the opposing expert. Worked as the expert for the U.S. Attorney's Office who handled the defense because Cino was an employee of the Department of Transportation, *Omogbehin v. Cino*, The United States District Court for the District of New Jersey, Case No. 1:06-cv-04581-JEI-JS

January 2009 to June 2009: Submitted two declarations regarding the search for and remediation of intellectual property from a former employer in a pre-litigation matter.

October 2007 to November 2007: Provided written testimony in the form of a declaration and an expert report opining on web-based postings of sensitive information in *Saffran, M.D., Ph.D., v. Boston Scientific Corporation,* The United States District Court for the Eastern District of Texas, Case No. 2:05-cv-00547-TJW

August 2005 to April 2007: Submitted multiple affidavits and expert reports. Testified in deposition and at trial as an expert witness in digital forensics on findings and opinions resulting from computer forensic analysis in a copyright infringement matter, *Merchant Transaction v. Nelcela Incorporated, et al.*, The United States District Court for the District of Arizona, Case No. 2:02-cv-01954-NVW

November 2006: Provided written testimony in the form of a certification regarding deletion of information from multiple computer systems in *Samsung America Inc. v. Park*, New Jersey Superior Court, Chancery Division, Case No. C-379-06

November 2005 to July 2006: Submitted multiple affidavits and expert reports regarding lost or destroyed evidence and analysis of several Windows and AIX UNIX computers. Testified at trial as an expert on findings and opinions resulting from investigation of computer evidence in *United States v. Duronio,* The United States District Court for the District of New Jersey, Case No. 2:02-cr-00933-JLL

August 2005 to December 2005: Submitted multiple affidavits related to cost shifting and presented opinions at court conference in *Quinby v. WestLB AG,* The United States District Court for the Southern District of New York, Case No. 1:04-cv-07406-WHP-HBP

July 2004 to January 2005: Provided written testimony in the form of declarations and expert reports, as well as oral testimony in deposition regarding computer forensic analysis of data in an intellectual property matter, *Judy DiBattisto, et al. v. PSS World Medical, Inc.*, The United States District Court for the District of Nevada, Case No. 2:03-cv-00998

AWARDS AND RECOGNITION

March 2014: Consulting Magazine, The Rising Stars of the Profession – 35 under 35

FAULKNER EXHIBIT 2 — MATERIALS CONSIDERED

Case Materials

All documents cited in my report that are not cited herein.

Forensic image of Ms. Chen's computer using a Logicube Falcon-Neo forensic imaging device dated November 19, 2020, by Unit 42.

An iTunes backup of Mayor Durkan's iPhone 8 Plus (Verizon), model: A1864, serial number: F17WDNB4JCLM dated August 29, 2019, located on the forensic image of Ms. Chen's computer.

A Cellebrite advanced logical data extraction of Mayor Durkan's iPhone 8 Plus (Verizon), model: A1864, serial number: F17WDNB4JCLM dated July 2, 2021, by Unit 42.

A Cellebrite full file system extraction of Mayor Durkan's iPhone 8 Plus (Verizon), model: A1864, serial number: F17WDNB4JCLM dated July 7, 2021, by Unit 42.

A Magnet ACQUIRE data extraction of Mayor Durkan's iPhone 8 Plus (FirstNet), model: A1897, serial number: FD1XR5Y8JCM2 dated September 18, 2020, by an "Information Security Engineer" with the City.

A Cellebrite advanced logical data extraction of Mayor Durkan's iPhone 8 Plus (FirstNet), model: A1897, serial number: FD1XR5Y8JCM2 dated November 19, 2020, by Unit 42.

A Cellebrite full file system extraction of Mayor Durkan's iPhone 8 Plus (FirstNet), model: A1897, serial number: FD1XR5Y8JCM2 dated July 7, 2021, by Unit 42.

An iTunes backup of Mayor Durkan's iPhone 11 (FirstNet), model: A2111, serial number: F4GCQQ6PN72Q, dated August 21, 2020, located on the forensic image of Ms. Chen's computer.

A Magnet ACQUIRE data extraction of Mayor Durkan's iPhone 11 (FirstNet), model: A2111, serial number: F4GCQQ6PN72Q, dated October 15, 2020, by an "Information Security Engineer" with the City.

A Cellebrite advanced logical data extraction of Mayor Durkan's iPhone 11 (FirstNet), model: A2111, serial number: F4GCQQ6PN72Q, dated November 19, 2020, by Unit 42.

A full file system extraction, using unc0ver jailbreak and forensic software from Belkasoft LLC, of Mayor Durkan's iPhone 11 (FirstNet), model: A2111, serial number: F4GCQQ6PN72Q, dated July 8, 2021, by Unit 42

Data collection from Mayor Durkan's iCloud account "durje.mos@gmail.com" using Magnet AXIOM Cloud and Elcomsoft Phone Breaker dated November 16, 2020, by Unit 42.

Data collection of account data and text messages in iCloud from Mayor Durkan's iCloud account "durje.mos@gmail.com" using Elcomsoft Phone Breaker dated September 9, 2021, by Unit 42.

An inspection on November 19, 2020, by Unit 42, of a Microsoft Surface Pro 4, serial number: 048165462053, which was described as the tablet Mayor Durkan uses from home for City-related work.

An inspection on November 19, 2020, by Unit 42, of a Microsoft Surface Pro 7, serial number: 030612294353, which was described as the tablet Mayor Durkan uses from the office for City-related work.

An extraction from Pinnacle, the centralized database that receives billing and usage information from cellular providers used by the City, containing records from the beginning of January 2020 through the end of August 2020 for Mayor Durkan's mobile phone number.

A Cellebrite advanced logical data extraction of Chief Best's iPhone XS Max, model: A1921, serial number: F2LZ5ANGKPHC, dated February 24, 2021, by ArcherHall.

A Cellebrite advanced logical data extraction of Chief Best's iPhone XS Max, model: A1921, serial number: F2LZ5ANGKPHC, dated November 8, 2021, by Unit42.

Forensic image of Tricia Colin's computer using a Logicube Falcon-Neo forensic imaging device dated October 22, 2021, by Epic.

An iTunes backup of Chief Best's iPhone 8 Plus, model: A1864, serial number: FD6W12T6JCLY, dated October 1, 2019, located on the forensic image of Tricia Colin's computer.

An iTunes backup of Chief Best's iPhone 6s Plus, model: A1687, serial number: F2LRMBLFGRWV, dated November 15, 2017, located on the forensic image of Tricia Colin's computer.

A document titled "Smartphone Backup Process."

Deposition Transcripts

Deposition Transcript of Carmen Best, dated November 9, 2021

Deposition Transcript of Mayor Jenny A. Durkan, dated December 8, 2021

Production Documents

SEA_00144252

SEA_00145700

SEA_00145708

SEA_00145710

"PLAINTIFFS' SECOND SET OF INTERROGATORIES TO DEFENDANT CITY OF SEATTLE **AND THE CITY'S OBJECTIONS AND FIRST SUPPLEMENTAL RESPONSES THERETO"** dated August 31, 2021.

Websites

https://support.apple.com/en-us/HT207428

FAULKNER EXHIBIT 2 — MATERIALS CONSIDERED

https://support.apple.com/en-us/HT202033

https://support.apple.com/guide/icloud/messages-mm0de0d4528d/icloud

https://developer.apple.com/documentation/corefoundation/1543542-cfabsolutetimegetcurrent

https://support.apple.com/en-us/HT201287

https://support.apple.com/guide/iphone/erase-iphone-iph7a2a9399b/14.0/ios/14.0

https://www.apple.com/legal/internet-services/icloud/en/terms.html

https://support.apple.com/guide/icloud/back-up-your-ios-and-ipados-device-mmab848634c8/icloud